Date: 2024

A Contract for Services

Independent Children's Rights and Advocacy Services

Between

The Secretary of State for Justice

And

Barnardo's

CONTENTS

Schedules

This Contract is dated: **2024**

PARTIES:

(1) THE SECRETARY OF STATE FOR JUSTICE of 102 Petty France, London, SW1H 9AJ acting as part of the Crown (the "**Authority**");

AND

(2) BARNARDO'S with registered company number 00061625 whose registered office is Barnardo House, Tanners Lane, Barkingside, Ilford, Essex, IG6 1QG (the "**Supplier**")

(each a "**Party**" and together the "**Parties**").

WHEREAS

A. On 15 August 2023, the Authority advertised on the UK e-notification service (reference 2023/S 000-023948), inviting prospective suppliers to submit proposals for the provision of independent children's rights and advocacy services at Secure Establishments.

B. Following a competitive tender process pursuant to the light touch regime, following the general principles of the open procedure, the Authority wishes to appoint the Supplier to provide independent children's rights and advocacy services at Secure Establishments and the Supplier agrees to provide those services in accordance with these terms and conditions.

NOW IT IS HEREBY AGREED:

A GENERAL

A1 Definitions and Interpretation

A1.1 Unless the context otherwise requires the following terms shall have the meanings given to them below:

"**Advocate**" means a member of the Supplier's Staff responsible for representing the views, wishes and needs of, and supporting, Children and Young People, who undertakes the advocacy Service tasks at the Secure Establishments in accordance with the Specification.

"**Advocacy Plan**" means the clearly documented plan agreed with the Child or Young Person that shows the agreed outcome(s) of advocacy support and the work Advocates agree to undertake with or on behalf of the Child or Young Person.

"**Affected Party**" means the Party seeking to claim relief in respect of a Force Majeure Event.

"**Affiliate**" means in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time.

"Annual Report" has the meaning given to it in Paragraph 3.1 of Schedule 10 (Performance Mechanism).

"**Anti-Malicious Software**" means software which scans for and identifies possible Malicious Software in the ICT Environment.

"**Approve**", "**Approval**" and "**Approved**" means the prior written consent of the Authority.

"**Assessment Tool**" means the modern slavery risk identification and management tool which can be found at: *https://supplierregistration.cabinetoffice.gov.uk/msat*

"**Associated Person**" means as it is defined in section 44(4) of the Criminal Finances Act 2017.

"**Authorised Representative**" means the Authority representative named in a CCN who is authorised to approve Changes.

"**Authority Cause**" means any material breach by the Authority of any of the Authority Responsibilities, except to the extent that such breach is:

(a) the result of any act or omission by the Authority to which the Supplier has given its prior consent; or

(b) caused by the Supplier, any Sub-Contractor or any Staff.

"**Authority Data**" means:

(a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are: (i) supplied to the Supplier by or on behalf of the Authority; or (ii) which the Supplier is required to generate, process, store or transmit pursuant to this Contract; and/or

(b) any Personal Data for which the Authority is the Controller; and/or

(c) any CYP Data (provided that the Parties agree and acknowledge that CYP Personal Data for which the Supplier is the Controller, that forms a part of CYP Data shall belong to the Child or Young Person, and the Authority shall have no right to receive or own any such CYP Personal Data except in accordance with clause H9.7 (Exit Management) or clause H10 (Knowledge Retention) or for the purposes of Safeguarding or to the extent that access to such information is reasonably required in connection with an audit under Clause F5 (Audit)).

"**Authority Equipment**" means the Authority's equipment, consumables, plant, materials and such other items provided to the Supplier for the delivery of the Services, which may include (but shall not necessarily be limited to) office furniture and certain office equipment.

"**Authority Premises**" means any premises owned, occupied or controlled by the Authority or any other Crown Body which are made available for use by the Supplier or its Sub-Contractors for provision of the Services.

"**Authority Responsibility**" means a responsibility of the Authority in respect of this Contract, set out in Paragraph 3 of Schedule 18 (Authority Responsibilities).

"**Authority Software**" means software which is owned by or licensed to the Authority (other than under or pursuant to this Contract) and which is or will be used by the Supplier for the purposes of providing the Services.

"**Authority System**" means the Authority's computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the Authority or the Supplier in connection with this Contract which is owned by or licensed to the Authority by a third party and which interfaces with the Supplier System or which is necessary for the Authority to receive the Services.

"**Authority Technical Security Guidance**" means the technical security guidance published by the Authority at: *https://security-guidance.service.justice.gov.uk/#cyber-and-technical-security-guidance*

"**Basware**" means Basware eMarketplace, the procurement software used by the Authority for its financial transactions.

"**BPSS**" means the Government's Baseline Personnel Security Standard for Government employees.

"**Breach of Security**" means an event which results in or could result in:

(a) any unauthorised access to or use of the Authority Data, the Services and/or the Information Management System; and/or

(b) the loss, corruption and/or unauthorised disclosure of any information or data (including Confidential Information and Authority Data), including any copies of such information or data, used by the Authority and/or the Supplier in connection with this Contract.

"**Break Option**" has the meaning given to it in clause A5.3.

"**BS 8555**" means the standard published to help organisations improve their environmental performance by the British Standards Institution.

"**Business Continuity Plan**" means the business continuity plan prepared by the Supplier pursuant to clause H6 and Schedule 11 (Business Continuity Plan), the draft version of which is set out in Annex A to Schedule 11, as amended from time to time in accordance with Schedule 11.

"**Case Management**" means the method of delivering the Services as described in the Specification at Schedule 1.

"**Case Management System**" means the system created and managed by the Supplier in the operation of the Services regarding individual Children and Young People, including (but not limited to) Live Case(s).

"**Case Management Data**" means the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are created by the Supplier in the operation of the Services regarding individual Children and Young People, including (but not limited to) Live Cases.

"**CCN**" means a contract change notice in the form set out in Schedule 3 (Change Control).

"**Certification Requirements**" means the requirements set out in Paragraph 5 of Schedule 6 (Information Security & Assurance).

"**Change**" means a change in any of the terms or conditions of this Contract.

"**Change in Law**" means any change in Law which affects the performance of the Services which comes into force after the Commencement Date.

"**CHECK Service Provider**" means an organisation which has been certified by the NCSC, holds "Green Light" status and is authorised to provide the IT Health Check services required by Paragraph 6.1 of Schedule 6 (Information Security & Assurance).

"**Child or Young Person**" means a child or young person accommodated within a Secure Establishment, and "**Children and Young People**" shall be construed accordingly.

"**Closed Case(s)"** means the casework relating to individual Children and Young People carried out by Advocates under the requirements of providing the Service, where either:

(a) the Child or Young Person has exited the secure estate (transfer between Secure Establishments does not amount to exit); or
(b) the matter which has led to the Child or Young Person requiring the Service has been resolved or come to a close.

"**Commencement Date**" means the date specified in Clause A5.1.

"**Commercially Sensitive Information**" means the information listed in Schedule 4 (Commercially Sensitive Information) comprising the information of a commercially sensitive nature (but not including the Publishable Performance Information) relating to:

(a) the Price; and/or

(b) the Supplier's business and investment plans

which the Supplier has informed the Authority would cause the Supplier significant commercial disadvantage or material financial loss if it was disclosed.

"**Comparable Supply**" means the supply of services to another customer of the Supplier which are the same or similar to any of the Services.

"**Confidential Information**" means any information which has been designated as confidential by either Party in writing or that ought to be considered as confidential (however it is conveyed or on whatever media it is stored) including information the disclosure of which would, or would be likely to, prejudice the commercial interests of any person or trade secrets or Intellectual Property Rights of either Party and all Personal Data. Confidential Information shall not include information which:

(a) was public knowledge at the time of disclosure otherwise than by breach of Clause D4 (Confidential Information);

(b) was in the possession of the receiving Party, without restriction as to its disclosure, before receiving it from the disclosing Party;

(c) is received from a third party (who lawfully acquired it) without restriction as to its disclosure; or

(d) is independently developed without access to the Confidential Information.

"**Contract**" means these terms and conditions, the attached Schedules and any other provisions the Parties expressly agree are included.

"**Contract Delivery Indicators**" or "**CDIs**" means the performance indicators set out in Annex A of Schedule 10 (Performance Mechanism).

"**Contract Year**" means any one of the following:

"**Contract Year 1**"	the period between the 1 July 2024 and 31 March 2025;
"**Contract Year 2**"	the period between the 1 April 2025 and 31 March 2026;
"**Contract Year 3**"	the period between the 1 April 2026 and 31 March 2027;
"**Contract Year 4**"	the period between the 1 April 2027 and 31 March 2028;
"**Contract Year 5**"	the period between the 1 April 2028 and 31 March 2029;
"**Contract Year 6**"	the period between the 1 April 2029 and 31 March 2030;
"**Contract Year 7**"	the period between the 1 April 2030 and 31 March 2031;
"**Contract Year 8**"	the period between the 1 April 2031 and 30 June 2031.

"**Contracting Authority**" means any contracting authority (other than the Authority) as defined in regulation 2 of the Regulations.

"**Contracts Finder**" means the Government's portal for public sector procurement opportunities.

"**Control**" means that a person possesses, directly or indirectly, the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and "**Controls**" and "**Controlled**" are interpreted accordingly.

"**Controller**" means as it is defined in the UK GDPR.

"**Copyright**" means as it is defined in s.1 of Part 1 Chapter 1 of the Copyright, Designs and Patents Act 1988.

"**CREST Service Provider**" means an organisation with a SOC Accreditation from CREST International.

"**Crown**" means the government of the UK (including the Northern Ireland Executive Committee and Northern Ireland Departments, the Scottish Executive and the National Assembly for Wales), including, but not limited to, Government ministers, Government

departments, Government offices and Government agencies and "**Crown Body**" is an emanation of the foregoing.

"**Cyber Essentials**" means the Cyber Essentials certificate issued under the Cyber Essentials Scheme.

"**Cyber Essentials Plus**" means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme.

"**Cyber Essentials Scheme**" means the Cyber Essentials scheme operated by the NCSC.

"**CYP Data**" means all data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are created by the Supplier in the operation of the Services regarding individual young people which can include (but is not limited to):

(a) CYP Personal Data; and

(b) Live Cases.

"**CYP Personal Data** " means Personal Data of individual Children and Young People.

"**Data Loss Event**" means any event which results, or may result, in unauthorised access to Personal Data held by the Supplier under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data breach.

"**DPA**" means the Data Protection Act 2018.

"**DPIA**" means a data protection impact assessment by the Controller carried out in accordance with s.3 of the UK GDPR and s.64 and s.65 of the DPA.

"**Data Protection Law**" means:

(a) all applicable UK Law relating to the processing of Personal Data and privacy, including the UK GDPR and the DPA to the extent it relates to Processing of Personal Data and privacy; and

(b) (to the extent that it applies) the EU GDPR.

"**Data Protection Officer**" means as it is defined in the UK GDPR.

"**Data Subject**" means as it is defined in the UK GDPR.

"**Data Subject Request**" means a request made by or on behalf of a Data Subject in accordance with rights granted pursuant to Data Protection Law to access their Personal Data.

"**Database Rights**" means rights in databases which are defined in s.3A of Part 1 Chapter 1 of the Copyright, Designs and Patents Act 1988.

"**Default**" means any breach of the obligations or warranties of the relevant Party (including abandonment of this Contract in breach of its terms, repudiatory breach or breach of a fundamental term) or any other default, act, omission, negligence or statement of the relevant Party or the Staff in connection with the subject-matter of this Contract and in respect of which such Party is liable to the other.

"Deliverable" means an item or feature delivered or to be delivered by the Supplier at or before a Milestone Date or at any other stage during the performance of this Contract.

"Detailed Mobilisation Plan" means the plan developed and revised from time to time in accordance with Paragraph 3 of Schedule 13 (Mobilisation Plan).

"**DOTAS**" means the Disclosure of Tax Avoidance Schemes rules which require a promotor of tax schemes to tell HMRC of any specified notifiable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act and as extended to NICs by the National Insurance (Application of Part 7 of the Finance Act 2004) regulations 2012, SI 2012/1868 made under section 132A of the Social Security Administration Act 1992.

"Due Diligence Information" any information supplied to the Supplier by or on behalf of the Authority prior to the Commencement Date.

"**EEA**" means the European Economic Area.

"**EIR**" means the Environmental Information Regulations 2004 (SI 2004/3391) and any guidance and/or codes of practice issued by the ICO or relevant Government department in relation to such regulations.

"Emergency Exit" means any termination of this Contract which is not an Ordinary Exit.

"Employees" means those persons employed by the Supplier (and/or any Sub-Contractor) wholly or mainly in the supply of the Services immediately before the end of the Term.

"**Employee Liability Information"** means the information to be provided by an employer pursuant to Regulation 11 of TUPE to a prospective employer in advance of a TUPE transfer.

"**End Date**" means the date specified in clause A5.1.

"**Establishment Service Cessation Notice**" and "**ESCN**" each take the meaning given to them at Clause C4.

"**Estimated Year 1 Price**" means the Fixed Fees payable in Contract Year 1 as set out in Schedule 2 (Payment Mechanism).

"**EU**" means the European Union.

"**EU GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of Personal Data (General Data Protection Regulation) as it has effect in EU law.

"**Exit Day**" means as it is defined in the Withdrawal Act.

"Exit Information" means the following:

(a) details of the Services;

(b) inventory of any Authority Data or Authority Equipment held;

(c) details of any third-party contracts or licenses used in the provision of the Services;

(d) list of any ongoing or threatened disputes in connection with the Services;

(e) TUPE Information;

(f) such other information as the Authority may reasonably require.

"Exit Plan" means the plan produced and updated by the Supplier during the Term in accordance with Schedule 15 (Exit Plan).

"Extended Staffing Vacancy" has the meaning given to it in Paragraph 1.4(A) of Schedule 2 (Payment Mechanism).

"Extended Staffing Vacancy Credit" has the meaning given to it in paragraph 1.4(B) of Schedule 2 (Payment Mechanism).

"**Fees Template**" means the fees template set out in Annex A of Schedule 2 (Fees Template) and updated in accordance with paragraph 3.8 of Schedule 2 and clause C4.4.

"**Financial Remedy**" takes the meaning given to it in Paragraph 8.1 of Schedule 10 (Performance Mechanism).

"**Financial Year**" means the period from 1st April each year to the 31st March the following year.

"**Fixed Costs**" means the costs identified as such in the Fees Template.

"**Fixed Fees**" means the Fixed Costs, Management Fee and the Operational Risk Payment, as set out in the Fees Template.

"**FOIA**" means the Freedom of Information Act 2000 and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the ICO in relation to such legislation.

"**Force Majeure Event**" means any event outside the reasonable control of either Party affecting its performance of its obligations under this Contract arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control and which are not attributable to any wilful act, neglect or failure to take reasonable preventative action by that Party, including acts of God, riots, war or armed conflict, acts of terrorism, acts of Government, local government or regulatory bodies, for flood, storm or earthquake, or disaster but excluding any industrial dispute relating to the Supplier or the Staff or any other failure in the Supplier's supply chain caused by the Covid 19 pandemic or the UK's exit from the EU.

"**General Anti-Abuse Rule**" means:

(a) the legislation in Part 5 of the Finance Act 2013; and

(b) any future legislation introduced into parliament to counteract tax advantages arising from abusive arrangements to avoid NICs.

"**General Change in Law**" means a Change in Law where the change is of a general legislative nature (including taxation or duties of any sort affecting the Supplier) or which affects or relates to a Comparable Supply.

"**Good Industry Practice**" means standards, practices, methods and procedures conforming to the Law and the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar type of undertaking under the same or similar circumstances.

"**Government**" means the government of the UK.

"**Government Buying Standards**" means the standards published here: *https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs*

"**Greening Government Commitments**" means the Government's policy to reduce its effects on the environment, the details of which are published here: *https://www.gov.uk/government/collections/greening-government-commitments*

"**Halifax Abuse Principle**" means the principle explained in the CJEU Case C-255/02 Halifax and others.

"**Higher Risk Sub-contractor**" means a Sub-Contractor which processes Authority Data where that data includes:

(a) the Personal Data of 1,000 or more individuals in aggregate during the Term; or

(b) any part of that data includes any of the following:

i) financial information relating to any person;
ii) any information relating to actual or alleged criminal offences;
iii) any information relating to vulnerable people;
iv) any information relating to social care;
v) any information relating to a person's employment;
vi) Special Category Personal Data;

(c) the Authority, at its discretion designates a Sub-Contractor as a Higher Risk Sub-contractor in any procurement document related to this Contract; or

(d) the Authority considers, at its discretion, that any actual or potential Processing carried out by the Sub-Contractor is high risk.

"**HMRC**" means HM Revenue & Customs.

"**ICO**" means the Information Commissioner's Office.

"**ICT Environment**" means the Authority System and the Supplier System.

"**Improvement Actions**" has the meaning given to it in Paragraph 6.1 of Schedule 10 (Performance Management).

"**Improvement Notice**" has the meaning given to it in Paragraph 5.1 of Schedule 10 (Performance Management).

"**Improvement Plan**" has the meaning given to it in Paragraph 6.1 of Schedule 10 (Performance Management).

"**Induction**" means the induction of a Child or Young Period to a Secure Establishment by the Supplier in accordance with section 1 of the Specification and the relevant Local Protocol.

"**Incident Management Process**" means the process which the Supplier shall implement immediately after it becomes aware of a Breach of Security which is intended to restore normal operations as quickly as possible, minimising any adverse effect on the Authority Data, the Authority, the Services and/or users of the Services and which shall be shall be prepared by the Supplier in accordance with paragraph 3 Information Security Approval Statement of Schedule 6 using the template set out in annex 3 of Schedule 6 (Information Security & Assurance).

"**Information**" has the meaning given under section 84 of the FOIA.

"**Information Assets**" means definable pieces of information stored in any manner which are determined by the Authority to be valuable and relevant to the Services.

"**Information Assurance Assessment**" means the set of policies, procedures, systems and processes which the Supplier shall implement, maintain and update in accordance with Paragraph 3 of Schedule 6 in order to manage, mitigate and, where possible, avoid information security risks including cyber-attacks, hacks, data leaks, Personal Data Breaches and/or theft and which shall be prepared by the Supplier using the template set out in Schedule 6 (Information Security & Assurance).

"**Information Management System**" means:

(a) those parts of the Supplier System, and those of the Premises, which the Supplier or its Sub-contractors use to provide the parts of the Service which require Processing Authority Data; and

(b) the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources).

"**Information Security Approval Statement**" means a notice issued by the Authority which sets out the information risks which the Supplier has identified as being associated with using the Information Management System and confirms that:

(a) the Authority is satisfied that the identified risks have been adequately and appropriately addressed;

(b) the Authority has accepted the residual risks; and

(c) the Supplier may use the Information Management System to process Authority Data.

"**Initial Term**" means the period from the Commencement Date to the End Date.

"**Intellectual Property Rights**" means:

(a) patents, utility models, inventions, trademarks, service marks, logos, design rights (whether registrable or otherwise), Database Rights, domain names, semi-conductor topography rights, rights in Internet domain names, Know-How, trade or business names, moral rights, the right to sue for passing off, trade secrets and other rights in Confidential Information, in each whether registrable or not in any country;

(b) applications for registration, and the right to apply for registration, for any of the rights listed in (a) that are capable of being registered in any country or jurisdiction; and

(c) all other rights having equivalent or similar effect in any country or jurisdiction.

"**ISO**" means the International Organisation for Standardisation.

"**ISO/IEC 14001**" means the family of standards related to environmental management published by the ISO.

"**ISO/IEC 27001**" means the family of standards related to information security management published by the ISO.

"**ISO/IEC 27002**" means the family of standards related to information security, cyber security and privacy protection published by the ISO.

"**ITEPA**" means the Income Tax (Earnings and Pensions) Act 2003.

"**IT Health Check**" means as it is defined in Paragraph 7.1(a) of Schedule 6.

"**Joint Controllers**" means as it is defined in Article 26 of the UK GDPR.

"**Key Personnel**" mean the people named in Schedule 14 (Key Personnel), if any, as may be determined by the Authority prior to the Commencement Date with reference to the Supplier's Tender.

"**Know-How**" means all information not in the public domain held in any form (including without limitation that comprised in or derived from drawings, data formulae, patterns, specifications, notes, samples, chemical compounds, biological materials, computer software, component lists, instructions, manuals, brochures, catalogues and process descriptions and scientific approaches and methods).

"**Law**" means any law, statute, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Supplier is bound to comply.

"**Law Enforcement Purposes**" means as it is defined in the DPA.

"**Live Case(s)**" means the casework relating to individual Children and Young People carried out by Advocates under the requirements of providing the Service, where either:

(c) the Child or Young Person has not yet exited the secure estate (transfer between Secure Establishments does not amount to exit); or

(d) where the matter which has led to the Child or Young Person requiring the Service is not yet resolved or come to a close and/or there are requirements under the Specification still to be actioned.

"**Local Protocols**" means the arrangements agreed between the Supplier and each Secure Establishment that enable and ensure the delivery of Services to Children and Young People within the rules and environments of each Secure Establishment, as described by and, once in place appended to, Schedule 12 (Local Protocols).

"**Losses**" means losses, liabilities, damages, costs, fines and expenses (including legal fees on a solicitor/client basis) and disbursements and costs of investigation, litigation, settlement, judgment interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty or otherwise.

"**Malicious Software**" means any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.

"**Management Fee**" means the fee(s) identified as such in the Fees Template.

"**Material Breach**" means a breach (including an anticipatory breach) which has a material effect on the benefit which the Authority would otherwise derive from a substantial or material portion of this Contract.

"**Medium Risk Sub-contractor**" means a Sub-Contractor which processes Authority Data where that data:

(a) includes the Personal Data of between 100 and 999 individuals (inclusive) in aggregate during the Term; and

(b) does not include Special Category Personal Data.

"Milestone" means an event or task described in the Mobilisation Plan which, if applicable, shall be completed by the relevant Milestone Date.

"Milestone Date" means the target date set out against the relevant Milestone in the Mobilisation Plan by which the Milestone must be achieved (to the Authority's reasonable satisfaction).

"Mitigation Actions" has the meaning given to it in Paragraph 1.4(A) of Schedule 2 (Payment Mechanism).

"Mitigation Costs" has the meaning given to it in Paragraph 1.4(A) of Schedule 2 (Payment Mechanism).

"Mobilisation Payment" means any payment due from the Authority to the Supplier in respect of the mobilisation and/or transition of the Services, to the extent such payment is due in accordance with Paragraph 2 of Schedule 2 (Payment Mechanism).

"**Mobilisation Period**" means the period starting on the Commencement Date ending on the Services Commencement Date, during which the Services will be mobilised in accordance with the Mobilisation Plan.

"**Mobilisation Plan**" means the Outline Mobilisation Plan or (if and when approved by the Authority in accordance with Paragraph 3 of Schedule 13) the Detailed Mobilisation Plan as updated in accordance with Paragraph 3.8 of Schedule 13 from time to time.

"**Modern Slavery Helpline**" means the point of contact for reporting suspicion, seeking help or advice and information on the subject of modern slavery available by telephone on 08000 121 700 or online at: *https://www.modernslaveryhelpline.org/report*

“**Month**” means calendar month.

“Monthly Data Return” has the meaning given to it in Clause 3.1 of Schedule 10 (Performance Mechanism).

“**Monthly Payment**” shall have the meaning given to it in Paragraph 1.1(A) of Schedule 2 (Payment Mechanism).

“**MSA**” means the Modern Slavery Act 2015.

“**National Referral Mechanism**” means the framework for identifying and referring potential victims of modern slavery and ensuring they receive the appropriate support, as published by the Government from time to time.

“**NCSC**” means the National Cyber Security Centre.

“**NICs**” means National Insurance Contributions.

“**Occasion of Tax Non-Compliance**” means:

(a) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 which is found on or after 1 April 2013 to be incorrect as a result of:

i) a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse principle or under any tax rules or legislation that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle;

ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to the Relevant Tax Authority under the DOTAS or any equivalent or similar regime; and/or

(b) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 gives rise on or after 1 April 2013 to a criminal conviction in any jurisdiction for tax related offences which is not spent at the Commencement Date or to a civil penalty for fraud or evasion.

"**Open Book Data**" means complete and accurate financial and non-financial information which is sufficient to enable the Authority to verify:

(a) the Price already paid or payable and the Price forecast to be paid during the remainder of the Term;

(b) the Supplier’s costs and manpower resources broken down against each element of the Services;

(c) the cost to the Supplier of engaging the Staff, including base salary, tax and pension contributions and other contractual employment benefits; and

(d) operational costs which are not included within the above, to the extent that such costs are necessary and properly incurred by the Supplier in the delivery of the Services;

(e) all interest, expenses and any other third party financing costs incurred in relation to the provision of the Services; and

(f) the profit achieved over the Term and annually.

"**Operational Risk Payment**" means the payment(s) identified as such in the Fees Template.

"**Operational Services Milestone**" means the milestone(s) set out in the Mobilisation Plan, the achievement of which will mark the end of the Mobilisation Period and trigger the Services Commencement Date.

"Optional Services" means any of the services described at section 6 of the Specification.

"Ordinary Exit" any termination of the whole or any part of this Contract which occurs:

(a) as a result of the Authority exercising the Break Option;

(b) pursuant to clause H1, H2, H3, H3A or H4 where the period of notice given by the Party serving notice to terminate pursuant to such clause is greater than or equal to six (6) months; or

(c) as a result of the expiry of the Term.

"Outline Mobilisation Plan" means the outline plan set out at Annex 1 of Schedule 13.

"**Outstanding Issues Notice**" has the meaning given to it in Paragraph 7.1 of Schedule 10 (Performance Management).

"**Performance Mechanism Trigger**" means a trigger set out in the table in paragraph 4.1 of Schedule 10 (Performance Mechanism) which, if met, gives rise to a remedy for the Authority as detailed in Schedule 10.

"**Performance Point**" means a point accrued by the Supplier as a result of a failure to meet a CDI, such points shall be calculated in accordance with Annex A to Schedule 10 (Performance Mechanism).

"**Performance Points Threshold**" means a threshold as set out in the table in paragraph 4.1 of Schedule 10 (Performance Mechanism) which, if met, gives rise to a remedy for the Authority as detailed in Schedule 10.

"**Performance Quarter**" means three (3) Month periods occurring from Services Commencement Date, grouped 1 April to 30 June, 1 July to 30 September, 1 October to 31 December and 1 January to 31 March applicable in the relevant Contract Year.

"**Personal Data**" means as it is defined in the UK GDPR.

"**Personal Data Breach**" means as it is defined in the UK GDPR.

"**Policies and Standards**" means the policies and standards referred to in Annex A of Schedule 16 (Policies and Standards), as amended, updated or added to from time to time.

"**Premises**" means the location where the Services are to be supplied set out in the Specification and/or Schedule 7 (Secure Establishments).

"**Price**" means the price (excluding any applicable VAT) payable to the Supplier by the Authority under this Contract, as set out in Schedule 2 (Payment Mechanism) for the full and proper performance by the Supplier of its obligations under this Contract. For the avoidance of doubt, the Price for each Contract Year shall be the aggregate of the Monthly Payments made in that Contract Year.

"**Price Adjustment Date**" has the meaning given to it in Paragraph 3.2 of Schedule 2 (Payment Mechanism).

"**Processing**" means as it is defined in Article 4 of the UK GDPR and "**Process**" is construed accordingly.

"**Processor**" means as it is defined in the UK GDPR.

"**Prohibited Act**" means:

(a) to directly or indirectly offer, promise or give any person working for or engaged by the Authority a financial or other advantage to:

i) induce that person to perform improperly a relevant function or activity; or

ii) reward that person for improper performance of a relevant function or activity;

(b) to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with this Contract;

(c) an offence:

i) under the Bribery Act 2010 (or any legislation repealed or revoked by such Act);

ii) under legislation or common law concerning fraudulent acts (including offences by the Supplier under Part 3 of the Criminal Finances Act 2017); or

iii) the defrauding, attempting to defraud or conspiring to defraud the Authority;

(d) any activity, practice or conduct which would constitute one of the offences listed under (c) above if such activity, practice or conduct has been carried out in the UK.

"**Protective Measures**" means appropriate technical and organisational measures designed to ensure compliance with obligations of the Parties arising under Data Protection Law and this Contract which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the measures adopted.

"**PSI 07/2016**" is the Prison Service Instruction published on 26th October 2016 relating to the searching of the person as amended from time to time and available at: https://www.gov.uk/government/publications/procedures-for-searching-people-psi-072016

"**PSI 10/2012**" is the Prison Service Instruction published on 26 March 2012 relating to the Conveyance and Possession of Prohibited Items and other Related Offences as amended from time to time and available at: https://www.gov.uk/government/publications/controlling-banned-prohibited-items-psi-102012

"**PSI 07/2014**" is the Prison Service Instruction published on 2nd June 2014 relating to security vetting as amended from time to time and available at: ttps://www.gov.uk/government/publications/security-vetting-psi-072014-pi-032014

"**Publishable Performance Information**" means any of the information in the Monthly Data Return or Quarterly Contract Management Report as it relates to a CDI where it is expressed as publishable in the table in Annex A of Schedule 10 (Performance Mechanism) which shall not constitute Commercially Sensitive Information.

"**Purchase Order**" the Authority's order for the supply of the Services.

"**Quality Standards**" means the quality standards published by BSI British Standards, the National Standards Body of the UK, the International Organisation for Standardization or other reputable or equivalent body (and their successor bodies) that a skilled and experienced operator in the same type of industry or business sector as the Supplier would reasonably and ordinarily be expected to comply with, and as may be further detailed in Schedule 1 (Specification).

"**Quarterly Contract Management Report**" has the meaning given to it in Paragraph 3.1 of Schedule 10 (Performance Mechanism).

"Reduced Performance" means an incident where the Supplier has:

(a) failed to operate in accordance with this Contract; or

(b) the performance of the Supplier of its obligations under this Contract has otherwise fallen below the standard reasonably required by the Authority.

"**Regulations**" means the Public Contracts Regulations 2015 (SI 2015/102).

"**Regulated Activity**" in relation to children shall have the same meaning as set out in Part 1 of Schedule 4 to the Safeguarding Vulnerable Groups Act 2006, and in relation to vulnerable adults shall have the same meaning as set out in Part 2 of Schedule 4 to the Safeguarding Vulnerable Groups Act 2006.

"**Regulatory Body**" means a Government department and regulatory, statutory and other entities, committees, ombudsmen and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in this Contract or any other affairs of the Authority.

"**Relevant Conviction**" means a conviction that is relevant to the nature of the Services or as listed by the Authority and/or relevant to the work of the Authority.

"**Relevant Requirements**" means all applicable Law relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State for Justice pursuant to section 9 of the Bribery Act 2010.

"**Relevant Tax Authority**" means HMRC or, if applicable, a tax authority in the jurisdiction in which the Supplier is established.

"**Remediation Plan**" means as it is defined in Paragraph 6.3(c)(i) of Schedule 6.

"**Replacement Supplier**" means any third-party supplier appointed by the Authority to supply any services which are substantially similar to any of the Services in substitution for any of the Services following the expiry, termination or partial termination of this Contract.

"**Request for Information**" means a request for information under the FOIA or the EIR.

"**Required Changes Register**" means the register within the Security Management Plan which is to be maintained and updated by the Supplier and which shall record each of the changes that the Supplier shall make to the Information Management System and/or the Security Management Plan as a consequence of the occurrence of any of the events set out in paragraph 4.2 of Schedule 6 together with the date by which such change shall be implemented and the date on which such change was implemented.

"**Restricted Status**" means a Child or Young Person who is convicted or on remand, whose escape would present a serious risk to the public and who is required to be held in designated secure accommodation, as determined by the Authority or a Secure Establishment.

"**Results**" means any guidance, specifications, reports, studies, instructions, toolkits, plans, data, drawings, databases, patents, patterns, models, designs or other material which is:

(a) prepared by or for the Supplier for use in relation to the performance of its obligations under this Contract; and/or

(b) the result of any work done by the Supplier or any Staff in relation to the provision of the Services,

but which shall not include any CYP Personal Data.

"**Risk Register**" means the risk register within the Information Assurance Assessment which is to be prepared and submitted for Approval in accordance with paragraph 3 of Schedule 6.

"ROPA" means the records of processing activities set out at Annex B of Schedule 9 as required under the UK GDPR and agreed between the Parties.

"**Safeguarding**" means protecting Children and Young Peoples' health, wellbeing and human rights, and enabling them to live free from harm, abuse and neglect.

"**Security Incident**" means the access to the ICT Environment by an unauthorised person for any reason or the unauthorised alteration of the functionality of the ICT Environment.

"**Secure Establishment(s)**" means either:

(a) Secure Training Centres; or

(b) Young Offender Institution,

where the Services are due to be delivered, as detailed in Schedule 7 (Secure Establishments) or the Detailed Mobilisation Plan.

"**Secure Training Centre**" means a secure training centre, which accommodates young people in custody, who are too vulnerable for a Young Offender Institution.

"**Security Management Plan**" means the plan prepared by the Supplier using the template in Annex 3 of Schedule 6, comprising:

(a) the Information Assurance Assessment;

(b) the Required Changes Register; and

(c) the Incident Management Process.

"**Security Policy Framework**" means the Government's security policy framework (available from the Cabinet Office's Government Security Secretariat) as updated from time to time.

"**Services Commencement Date**" has the meaning given to it in Clause A5.2.

"**Services**" means the services set out in Schedule 1 (including any modified or alternative services). "**Advocacy Services**" shall have the same meaning.

"**SME**" means an enterprise falling within the category of micro, small and medium-sized enterprises defined by the European Commission's Recommendation of 6 May 2003 available at: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:en:PDF*

"**Special Category Personal Data**" means the categories of Personal Data set out in article 9(1) of the UK GDPR.

"**Specific Change in Law**" means a Change in Law that relates specifically to the business of the Authority and which would not affect a Comparable Supply.

"**Specification**" means the description of the Services to be supplied under this Contract as set out in Schedule 1 (Specification).

"**SSCBA**" means the Social Security Contributions and Benefits Act 1992.

"**Staff**" means all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any of its Sub-Contractors engaged in the performance of the Supplier's obligations under this Contract.

"**Sub–Contract**" means a contract between two or more suppliers, at any stage of remoteness from the Authority in a sub-contracting chain, made wholly or substantially for the purpose of performing (or contributing to the performance of) the whole or any part of this Contract and "**Sub-Contractor**" shall be construed accordingly.

"**Sub-processor**" means any third party appointed to process Personal Data on behalf of the Supplier related to this Contract.

"**Supplier Equipment**" means the Supplier's equipment, consumables, plant, materials and such other items supplied and used by the Supplier in the delivery of the Services (including, but not limited to any IT equipment required for the Delivery of the Services).

"**Supplier Proposal**" means the Supplier's proposal(s), including any method statement(s) describing how the Supplier will achieve the outcomes set out in the Specification, in relation to the performance of the Services, supplied by the Supplier as part of the Tender and inserted at Annex A of Schedule 1.

"**Supplier Software**" means software, which is proprietary to the Supplier, including software which is or will be used by the Supplier for the purposes of providing the Services and which is set out in Schedule 5 (Supplier and Third Party Software).

"**Supplier System**" means the information and communications technology system used by the Supplier in performing the Services including the Software, the Equipment and related cabling (but excluding the Authority System).

"**Tender**" means the Supplier's tender submitted in response to the Authority's invitation to suppliers for offers to supply the Services.

"**Term**" means the period from the Commencement Date to the End Date or such earlier date of termination or partial termination of this Contract in accordance with the Law or this Contract.

"Termination Assistance Notice" a written notice provided by the Authority to the Supplier requiring the Supplier to provide the Termination Services, serviced at least four (4) months prior to the date of termination or expiry of this Contract or as soon as reasonably practicable (but in any event, not later than one (1) month) following the service by either Party of a termination notice.

"Termination Assistance Period" in relation to a Termination Assistance Notice, the period specified in the Termination Assistance Notice for which the Supplier is required to provide the Termination Services, as such period may be extended by reasonable request of the Authority.

"Termination Services" the services and activities to be performed by the Supplier pursuant to the Exit Plan, and any other Services required further to clause H9.2.

"**Third Party IP Claim**" has the meaning given to it in Clause E1.5.

"**Third Party Software**" means software which is proprietary to any third party which is or will be used by the Supplier to provide the Services including the software and which is specified as such in Schedule 5 (Supplier and Third Party Software).

"**TUPE**" means the Transfer of Undertakings (Protection of Employment) Regulations 2006.

"**TUPE Information**" means the information set out in Paragraph 2.1 of Schedule 19 (Staff Transfers).

"**Unit Visit**" means a visit made by the Supplier to a residential unit of a Secure Establishment, in accordance with paragraph 1.5 of the Specification and the relevant Local Protocol.

"**UK**" means United Kingdom.

"**UK GDPR**" means the UK General Data Protection Regulation.

"**Valid Invoice**" means an invoice containing the information set out in Clause C1.3 or C1.4, which has not been disputed by the Authority.

"**VAT**" means value added tax charged or regulated in accordance with the Value-Added Tax Act 1994.

"**VCSE**" means a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives.

"**Welsh Language Scheme**" means the Authority's Welsh language scheme as amended from time to time and available at: http://www.justice.gov.uk/publications/corporate-reports/moj/2010/welsh-language-scheme

"**Withdrawal Act**" means the European Union (Withdrawal) Act 2018.

"**Working Day**" means a day (other than a Saturday or Sunday) on which banks are open for general business in the City of London.

"**Young Offender Institution**" means a young offender institution which accommodates young people in custody.

A1.2 In this Contract, unless the context implies otherwise:

(a) the singular includes the plural and vice versa unless the context requires otherwise;

(b) words importing the masculine include the feminine and the neuter;

(c) reference to a clause is a reference to the whole of that clause unless stated otherwise;

(d) references to a person include natural persons, a company, body corporate, corporation, unincorporated association, firm, partnership or other legal entity or central Government body;

(e) the words "other", "in particular", "for example", "including" and similar words shall not limit the generality of the preceding words and shall be construed as if they were immediately followed by the words "without limitation";

(f) headings are included for ease of reference only and shall not affect the interpretation or construction of this Contract;

(g) the annexes and Schedules form an integral part of this Contract and have effect as if set out in full in the body of this Contract. A reference to this Contract includes the annexes and Schedules;

(h) a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time;

(i) references to this Contract are references to this Contract as amended from time to time; and

(j) any reference in this Contract which immediately before Exit Day was a reference to (as it has effect from time to time):

(i) any EU regulation, EU decision, EU tertiary legislation or provision of the EEA agreement ("**EU References**") which is to form part of

domestic law by application of section 3 of the Withdrawal Act shall be read as a reference to the EU References as they form part of domestic law by virtue of section 3 of the Withdrawal Act as modified by domestic law from time to time; and

(ii) any EU institution or EU authority or other such EU body shall be read as a reference to the UK institution, authority or body to which its functions were transferred.

A1.3 In the event of any inconsistency between the terms of this Contract and any other document referred to herein, such conflict shall, save where expressly provided otherwise, be determined with the following order of precedence:

(a) Schedule 1 (Specification), excluding the Supplier Proposal at Annex A;

(b) Schedule 2 (Payment Mechanism);

(c) the terms and conditions of this Contract;

(d) the Schedules, other than Schedule 1 (Specification) and Schedule 2 (Payment Mechanism;

(e) any other documents referred to in this Contract;

(f) the Supplier Proposal.

A2 Authority Obligations

A2.1 Save as otherwise expressly provided, the Authority's obligations under this Contract are the Authority's obligations in its capacity as a contracting counterparty and nothing in this Contract operates as an obligation upon, or in any other way fetters or constrains, the Authority in any other capacity.

A2.2 The Authority shall use reasonable endeavours to comply with or perform the Authority Responsibilities.

A3 Supplier's Status

A3.1 The Supplier is an independent contractor and nothing in this Contract creates a contract of employment, a relationship of agency or partnership or a joint venture between the Parties and accordingly neither Party is authorised to act in the name of, or on behalf of, or otherwise bind the other Party save as expressly permitted by this Contract.

A3.2 The Supplier shall not (and shall ensure that any other person engaged in relation to this Contract shall not) say or do anything that might lead another person to believe that the Supplier is acting as the agent or employee of the Authority.

A4 Mistakes in Information

The Supplier is responsible for the accuracy of all drawings, documentation and information supplied to the Authority by the Supplier in connection with the Services

and shall pay the Authority any extra costs occasioned by any discrepancies, errors or omissions therein.

A5 Term

A5.1 The Contract starts on the date on which it is entered into (the "**Commencement Date**") and ends on 30 June 2031 (the "**End Date**") unless it is terminated early in accordance with this Contract.

A5.2 The Supplier shall commence provision of the Services in accordance with the requirements of this Contract from 1 July 2024, unless:

(a) the Operational Services Milestone(s) has or have not been met to the Authority's reasonable satisfaction by 1 July 2024, in which case the Supplier shall commence provision of the Services on the date on which the Operational Services Milestone(s) has or have been met to the Authority's reasonable satisfaction or such other date, or subject to such conditions as the Authority may reasonably require; or

(b) the Authority notifies the Supplier in writing that the Services shall commence on an alternative later date, in which case the Services shall commence on such alternative later date,

(the "**Services Commencement Date**").

A5.3 The Authority may, in its sole discretion, terminate this Contract for convenience on the fifth (5th) anniversary of the Commencement Date by giving the Supplier no less than three (3) months' written notice to expire on or before the fifth (5th) anniversary of the Commencement Date (the "**Break Option**").

B THE SERVICES

B1 Basis of this Contract

B1.1 In consideration of the Supplier's performance of its obligations under this Contract the Authority shall pay the Supplier the Price in accordance with clause C1.

B1.2 The terms and conditions in this Contract apply to the exclusion of any other terms and conditions the Supplier seeks to impose or incorporate, or which are implied by trade, custom, practice or course of dealing.

B1A Mobilisation Plan

B1A.1 The Parties shall comply with the provisions of Schedule 13 (Mobilisation Plan) in relation to the agreement and maintenance of the Detailed Mobilisation Plan.

B1A.2 The Supplier shall:

(a) comply with the Mobilisation Plan; and

(b) ensure that each Milestone is achieved (to the Authority's reasonable satisfaction) on or before its Milestone Date.

B1A.3 If the Supplier becomes aware that there is, or there is reasonably likely to be, a delay in the achievement of a Milestone by its Milestone Date or the design, development, testing or implementation of a Deliverable by the relevant date set out in the Mobilisation Plan, the Supplier shall promptly notify the Authority in writing, and shall use all reasonable endeavours to eliminate or mitigate the consequences of any delay or anticipated delay.

B2 Delivery of the Services

B2.1 The Supplier shall at all times comply with the Quality Standards and, where applicable, shall maintain accreditation with the relevant Quality Standards authorisation body. To the extent that the standard of the Service has not been specified in this Contract, the Supplier shall agree the relevant standard of the Services with the Authority prior to the supply of the Services and, in any event, the Supplier shall perform its obligations under this Contract in accordance with the Law and Good Industry Practice and the Supplier Proposal.

B2.2 The Supplier acknowledges that the Authority relies on the skill and judgment of the Supplier in the supply of the Services and the performance of the Supplier's obligations under this Contract.

B2.3 The Supplier shall:

(a) ensure that all Staff supplying the Services do so with all due skill, care and diligence and shall possess such qualifications, skills and experience as are necessary for the proper supply of the Services;

(b) ensure that all Staff are properly managed and supervised;

(c) comply with the standards and requirements set out in Schedule 8 and Local Protocols;

(d) comply with the Policies and Standards;

(e) prepare and provide to the Authority the information and reports in connection with Services and this Contract as are set out in the Specification, or as the Authority otherwise reasonably requires from time to time, at such frequency as set out in the Specification or as reasonably required by the Authority; and

(f) at all times collaborate and work in good faith with any third party contractor of the Authority acting at the Secure Establishments.

B2.4 If the Specification includes installation of equipment the Supplier shall notify the Authority in writing when it has completed installation. Following receipt of such notice, the Authority shall inspect the installation and shall, by giving notice to the Supplier:

(a) accept the installation; or

(b) reject the installation and inform the Supplier why, in the Authority's reasonable opinion, the installation does not satisfy the Specification.

B2.5 If the Authority rejects the installation pursuant to clause B2.4 (b), the Supplier shall immediately rectify or remedy any defects and if, in the Authority's reasonable opinion,

the installation does not, within 2 Working Days or such other period agreed by the Parties, comply with the Specification, the Authority may terminate this Contract with immediate effect.

B2.6 The installation is complete when the Supplier receives a notice issued by the Authority in accordance with clause B2.4 (a). Notwithstanding acceptance of any installation in accordance with clause B2.4 (a), the Supplier is solely responsible for ensuring that the Services and the installation conform to the Specification. No rights of estoppel or waiver shall arise as a result of the acceptance by the Authority of the installation.

B2.7 During the Term, the Supplier shall:

(a) at all times have all licences, approvals and consents necessary to enable the Supplier and Staff to carry out the installation;

(b) provide all tools and equipment (or procure the provision of all tools and equipment) necessary for completion of the installation;

(c) not, in delivering the Services, in any manner endanger the safety or convenience of the public.

B2.8 The Authority may inspect the manner in which the Supplier supplies the Services at the Premises during normal business hours on reasonable notice. The Supplier shall provide at its own cost all such facilities as the Authority may reasonably require for such inspection. In this clause B2, Services include planning or preliminary work in connection with the supply of the Services.

B2.9 If reasonably requested to do so by the Authority, the Supplier shall co-ordinate its activities in supplying the Services with those of the Authority and other contractors engaged by the Authority.

B2.10 The Supplier shall supply the Services in a timely manner, and at all times within any times specified for the delivery of such Services in the Specification, Detailed Mobilisation Plan or CDIs. If the Supplier fails to supply the Services within the time so specified, the Authority is released from any obligation to pay for such Services without prejudice to any other rights and remedies of the Authority.

B2.11 If the Authority informs the Supplier in writing that the Authority reasonably believes that any part of the Services do not meet the requirements of this Contract or differs in any way from those requirements, and this is not as a result of a default by the Authority, the Supplier shall at its own expense re-schedule and carry out the Services in accordance with the requirements of this Contract within such reasonable time as may be specified by the Authority.

B2.12 If, in delivering the Services, the Supplier is required to visit Authority Premises which are prisons, the Supplier shall comply with Schedule 7.

B3 Supplier Equipment

B3.1 The Supplier shall provide all the Supplier Equipment and resource necessary for the supply of the Services.

B3.2 The Supplier shall not deliver any Supplier Equipment to, or begin any work on, the Premises without Approval (such Approval may be set out in the Specification).

B3.3 All Supplier Equipment brought onto the Premises is at the Supplier's own risk and the Authority has no liability for any loss of or damage to any Equipment unless the Supplier demonstrates that such loss or damage was caused or contributed to by the Authority's Default. The Supplier shall provide for the haulage or carriage thereof to the Premises and the removal of Supplier Equipment when no longer required at its sole cost.

B3.4 Supplier Equipment brought onto the Premises remains the property of the Supplier.

B3.5 If the Authority reimburses the cost of any Supplier Equipment to the Supplier the Supplier Equipment shall become the property of the Authority and shall on request be delivered to the Authority as directed by the Authority. The Supplier shall keep a full and accurate inventory of all and such Authority Equipment and deliver that inventory to the Authority on request and on completion of the Services.

B3.6 The Supplier shall maintain all Supplier Equipment in a safe, serviceable and clean condition.

B3.7 The Supplier shall, at the Authority's written request, at its own cost and as soon as reasonably practicable:

(a) remove immediately from the Premises Supplier Equipment which is, in the Authority's opinion, hazardous, noxious or not supplied in accordance with this Contract; and

(b) replace such item with a suitable substitute item of Supplier Equipment.

B3.8 Within 20 Working Days of the end of the Term, the Supplier shall remove the Supplier Equipment together with any other materials used by the Supplier to supply the Services and shall leave the Premises in a clean, safe and tidy condition. The Supplier shall make good any damage to those Premises, Authority Equipment and any fixtures and fitting in the Premises which is caused by the Supplier or Staff.

B3.9 The Supplier shall not, at any time during the Term or during any Termination Assistance Period, bring onto the Premises any items that are expressly prohibited, either in the Specification (as such list may be updated by the Authority giving writing notice to the Supplier form time to time) or as otherwise notified by the Authority to the Supplier from time to time. The Supplier acknowledges that the Authority reserves the right to refuse access of any item to the Premises.

B4 Key Personnel

B4.1 The Supplier acknowledges that Key Personnel are essential to the proper provision of the Services.

B4.2 Key Personnel shall not be released from supplying the Services without Approval except by reason of long-term sickness, maternity leave, paternity leave or termination of employment or other similar extenuating circumstances.

B4.3 The Authority may interview and assess any proposed replacement for Key Personnel and any replacements to Key Personnel are subject to Approval. Such replacements shall be of at least equal status, experience and skills to Key Personnel being replaced and be suitable for the responsibilities of that person in relation to the Services.

B4.4 The Authority shall not unreasonably withhold approval under clauses B4.2 or B4.3 and such approval is conditional on appropriate arrangements being made by the Supplier to minimise any adverse effect on the Services which could be caused by a change in Key Personnel.

B5 Staff

B5.1 The Authority may, by notice to the Supplier, refuse to admit onto, or withdraw permission to remain on, the Authority's Premises:

(a) any member of the Staff; or

(b) any person employed or engaged by any member of the Staff

whose admission or continued presence would, in the Authority's reasonable opinion, be undesirable.

B5.2 The Authority shall maintain the security of the Authority's Premises in accordance with its standard security requirements, including Prison Rules 1999 Part III, the Prison (Amendment) Rules 2005, the Young Offender Institute Rules 2000 Part III and the Young Offender Institute (Amendment) Rules 2008, and the Secure Training Centre Rules 1998, available to the Supplier on request. The Supplier shall comply with all security requirements of the Authority while on the Authority's Premises, and ensure that all Staff comply with such requirements.

B5.3 The Authority may search any persons or vehicles engaged or used by the Supplier at the Authority's Premises.

B5.4 At the Authority's written request, the Supplier shall, at its own cost, provide a list of the names, addresses, national insurance numbers and immigration status of all people who may require admission to the Authority's Premises, specifying the capacities in which they are concerned with this Contract and giving such other particulars as the Authority may reasonably request.

B5.5 The Supplier shall ensure that all Staff who are delivering the Services, or who have access to the Authority's Premises, the Authority System or the Authority Data:

(a) are appropriately qualified, trained and experienced to provide the Services with all reasonable skill, care and diligence;
(b) comply with all reasonable requirements of the Authority concerning conduct at Authority Premises; and
(c) have been cleared in accordance with the BPSS and otherwise vetted in accordance with Good Industry Practice.

B5.6 The Supplier shall co-operate with any investigation relating to security carried out by the Authority or on behalf of the Authority and, at the Authority's request:

(a) use reasonable endeavours to make available any Staff requested by the Authority to attend an interview for the purpose of an investigation; and

(b) provide documents, records or other material in whatever form which the Authority may reasonably request or which may be requested on the Authority's behalf, for the purposes of an investigation.

B5.7 The Supplier shall comply with PSI 10/2012 as amended from time to time and available from the Authority on request.

B5.8 The Supplier shall be liable at all times for all acts or omissions of the Staff so that any act or omission of a member of Staff which results in a Default under this Contract shall be a Default of the Supplier.

B5.9 Without prejudice to clause G3, the Supplier or where relevant its Sub-Contractors shall at all times be responsible for all costs, contributions and liabilities associated with the Staff, including but not limited to pension contributions, NICs and redundancy payments.

B5.10 The Supplier shall comply with its requirements as an employer under the Pensions Act 2008 and all associated legislation in relation to all Staff.

B6 Due Diligence

B6.1 Save as the Authority may otherwise direct, the Supplier is deemed to have inspected the Premises before submitting its Tender and to have completed due diligence in relation to all matters connected with the performance of its obligations under this Contract.

B6.2 The Supplier warrants that it has made its own enquiries to satisfy itself as to the accuracy and adequacy of the Due Diligence Information.

B6.3 The Supplier shall not be excused from the performance of any of its obligations under this Contract on the grounds of, nor shall the Supplier be entitled to recover any additional costs or charges, arising as a result of any failure by the Supplier to carry out due diligence in relation to the Premises or to satisfy itself as to the accuracy and/or adequacy of the Due Diligence Information.

B7 Licence to Occupy

B7.1 Any land or Premises made available from time to time to the Supplier by the Authority in connection with this Contract are on a non-exclusive licence basis free of charge and are used by the Supplier solely for the purpose of performing its obligations under this Contract. The Supplier has the use of such land or Premises as licensee and shall vacate the same on termination of this Contract.

B7.2 The Supplier shall limit access to the land or Premises to such Staff as is necessary for it to perform its obligations under this Contract and the Supplier shall co-operate (and ensure that its Staff co-operate) with other persons working concurrently on such land or Premises as the Authority may reasonably request.

B7.3 If the Supplier requires modifications to the Authority's Premises such modifications are subject to Approval and shall be carried out by the Authority at the Supplier's cost.

B7.4 The Supplier shall (and shall ensure that any Staff on the Authority's Premises shall) observe and comply with such rules, regulations and requirements (including those relating to security arrangements) as may be in force from time to time, including but

not limited to those set out in Schedule 7 (Secure Establishments), for the conduct of personnel when on the Authority's Premises as determined by the Authority.

B7.5 The Contract does not create a tenancy of any nature in favour of the Supplier or its Staff and no such tenancy has or shall come into being and, notwithstanding any rights granted pursuant to this Contract, the Authority may use the Premises owned or occupied by it in any manner it sees fit.

B8 Authority Equipment

B8.1 All Authority Equipment is and remains the property of the Authority and the Supplier irrevocably licenses the Authority and its agents to enter any Premises of the Supplier during normal business hours on reasonable notice to recover any such Authority Equipment.

B8.2 The Supplier does not have a lien or any other interest on the Authority Equipment and the Supplier at all times possesses the Authority Equipment as fiduciary agent and bailee of the Authority. The Supplier shall take all reasonable steps to ensure that the title of the Authority to the Authority Equipment and the exclusion of any such lien or other interest are brought to the notice of all Sub-Contractors and other appropriate persons and shall, at the Authority's request, store the Authority Equipment separately and ensure that it is clearly identifiable as belonging to the Authority.

B8.3 The Authority Equipment is deemed to be in good condition when received by or on behalf of the Supplier unless the Supplier notifies the Authority otherwise within 5 Working Days of receipt.

B8.4 Save where otherwise set out in the Specification or otherwise agreed between the Parties, and subject to clause B8.6 below, the Authority shall maintain the Authority Equipment in reasonable order and condition (excluding fair wear and tear) and the Supplier shall use the Authority Equipment solely in connection with this Contract and for no other purpose without Approval.

B8.5 The Supplier shall ensure the security of all the Authority Equipment whilst in its possession, either on the Premises or elsewhere during the supply of the Services, in accordance with the Authority's reasonable security requirements as required from time to time.

B8.6 The Supplier is liable for all loss of or damage to the Authority Equipment, unless such loss or damage was caused by the Authority's negligence. The Supplier shall inform the Authority immediately of becoming aware of any defects appearing in, or losses or damage occurring to, the Authority Equipment.

B9 Offers of Employment

B9.1 Neither Party shall, directly or indirectly, solicit or procure (otherwise than by general advertising or under TUPE), any employees or contractors (including the Staff) of the other Party who are directly employed or engaged in connection with the provision of the Services while such persons are employed or engaged and for a period of 6 Months thereafter.

B9.2 If either Party breaches the clause B9.1, it shall pay the other Party a sum equivalent to 20% of the annual base salary payable by the Party in breach in respect of the first year of the person's employment.

B9.3 The Parties hereby agree that the sum specified in clause B9.2 is a reasonable pre-estimate of the loss and damage which the Party not in breach would suffer if there was a breach of clause B9.1.

B10 Employment

B10.1 The Parties will comply with the provisions of Schedule 19.

B11 Safeguarding children and vulnerable adults

B11.1 The Parties acknowledge that the Supplier is a Regulated Activity supplier with ultimate responsibility for the management and control of the Regulated Activity provided under this Contract and for the purposes of the Safeguarding Vulnerable Groups Act 2006.

B11.2 The Supplier shall:

(a) ensure that all individuals engaged in Regulated Activity are subject to a valid enhanced disclosure check for regulated activity undertaken through the Disclosure and Barring Service (DBS);
(b) monitor the level and validity of the checks under this clause B11.2 for each member of Staff;
(c) not employ or use the services of any person who is barred from, or whose previous conduct or records indicate that they would not be suitable to carry out Regulated Activity or who may otherwise present a risk to Children and Young People.

B11.3 The Supplier warrants that at all times for the purposes of this Contract it has no reason to believe that any person who is or will be employed or engaged by the Supplier in the provision of the Services is barred from the activity in accordance with the provisions of the Safeguarding Vulnerable Groups Act 2006 and any regulations made thereunder.

B11.4 The Supplier shall immediately notify the Authority of any information that it reasonably requests to enable it to be satisfied that the obligations of this clause B11 have been met.

B11.5 The Supplier shall refer information about any person carrying out the Services to the DBS where it removes permission for such person to carry out the Services (or would have, if such person had not otherwise ceased to carry out the Services) because, in its opinion, such person has harmed or poses a risk of harm to the Children and Young People.

B11.6 The Supplier shall, and shall procure that the Staff shall, comply with the National Referral Mechanism, as more particularly described in the Specification.

B12 Optional Services

B12.1 The Authority may require the Supplier to provide any or all of the Optional Services at any time by giving notice to the Supplier in writing. The Supplier acknowledges that the Authority is not obliged to take any Optional Services from the Supplier and that nothing shall prevent the Authority from receiving services that are the same as or similar to the Optional Services from any third party.

B12.2 If a Change Request Form set out in Schedule 3 is submitted, the Supplier shall, as part of the impact assessment of the Change provided by the Supplier provide details of the impact (if any) that the proposed Change will have on the relevant Optional Services.

B12.3 Following receipt of the Authority's notice pursuant to clause B12.1:

(a) the Parties shall document the inclusion of the relevant Optional Services within the Services in accordance with Clause F4 (Change), modified to reflect the fact that the terms and conditions on which the Supplier shall provide the relevant Optional Services have already been agreed;

(b) if required by the Authority, the Supplier shall produce or update any existing Mobilisation Plan for the relevant Optional Services;

(c) any additional charges for the Optional Services shall be incorporated in the Price; and

(d) the Supplier shall, from the date agreed with the Authority, provide the relevant Optional Services to meet or exceed the applicable Contract Delivery Indicators in respect of the Optional Services.

B13 Continuous Improvement

B13.1 The Supplier shall use reasonable endeavours throughout the duration of this Contract to identify areas where the Services can be improved or delivered for better value for money. Any improvements identified in accordance with this clause B13.1 shall be notified by the Supplier to the Authority in writing and, to the extent that the Authority approves the proposed improvement, shall be implemented into this Contract in accordance with clause F4 (Change).

C PAYMENT

C1 Payment and VAT

C1.1 The Supplier shall submit invoices to the Authority in accordance with this clause C1 and Schedule 2.

C1.2 The Authority issues Purchase Orders using Basware and, unless Approved otherwise, the Supplier shall, when invited, register on Basware.

C1.3 If the Supplier registers on Basware, a Valid Invoice is an invoice issued through Basware, unless the invoice contains:

(a) additional lines not included in the relevant Purchase Order;

(b) line descriptions which have been materially altered so that they no longer match the equivalent description in the relevant Purchase Order; or

(c) Prices and/or volumes which have been increased without Approval.

C1.4 If, with Approval, the Supplier does not register on Basware, a Valid Invoice is an invoice which complies with clauses C1.5 to C1.7.

C1.5 Other than invoices submitted through Basware, all invoices submitted to the Authority must clearly state the word 'invoice' and contain:

(a) a unique identification number (invoice number);

(b) the Supplier's name, address and contact information;

(c) the name and address of the department/agency in the Authority with which the Supplier is working;

(d) a clear description of the Services being invoiced for;

(e) the date the Services were provided;

(f) the date of the invoice;

(g) the amount being charged;

(h) VAT amount if applicable;

(i) the total amount owed;

(j) the Purchase Order number; and

(k) the amount of the invoice in sterling or any other currency which is Approved.

C1.6 Other than invoices submitted through Basware, all invoices submitted to the Authority must meet the following criteria:

(a) email size must not exceed 4mb;

(b) one invoice per file attachment (PDF). Multiple invoices can be attached as separate files;

(c) any supporting information, backing data etc. must be contained within the invoice PDF file;

(d) not contain any lines for items which are not on the Purchase Order;

(e) replicate, as far as possible, the structure of and the information contained in the Purchase Order in respect of the number of lines, line descriptions, price and quantity; and

(f) if required by the Authority, be submitted in a structured electronic invoice in an Electronic Data Interchange or XML formats.

C1.7 Other than invoices submitted through Basware, all invoices submitted to the Authority must, if requested by the Authority, include:

(a) timesheets for Staff engaged in providing the Services signed and dated by the Authority's representative on the Premises on the day;

(b) the name of the individuals to whom the timesheet relates and hourly rates for each;

(c) identification of which individuals are Supplier's Staff and which are Sub-Contractors' staff;

(d) the address of the Premises and the date on which work was undertaken;

(e) the time spent working on the Premises by the individuals concerned;

(f) details of the type of work undertaken by the individuals concerned;

(g) details of plant or materials operated and on standby;

(h) separate identification of time spent travelling and/or meal or rest breaks; and

(i) if appropriate, details of journeys made and distances travelled.

C1.8 The Authority shall not pay an invoice which is not a Valid Invoice.

C1.9 The Supplier acknowledges that the Price is the entire price payable by the Authority to the Supplier in respect of the Services and include, without limitation, any royalties, consents, licence fees, supplies and all consumables used by the Supplier, travel costs, accommodation expenses and the cost of Staff. The Authority shall not pay the Supplier's overhead costs unless Approved and overhead costs include, without limitation: facilities, utilities, insurance, tax, head office overheads, indirect staff costs and other costs not specifically and directly ascribable solely to the provision of the Services.

C1.10 NOT USED.

C1.11 NOT USED.

C1.12 NOT USED.

C1.13 The Supplier may not claim expenses unless they are Approved, clearly identified and supported by original receipts.

C1.14 If the Authority pays the Supplier prior to the submission of a Valid Invoice this payment is on account of and deductible from the next payment to be made.

C1.15 If any overpayment has been made or the payment or any part is not supported by a Valid Invoice the Authority may recover this payment against future invoices raised or directly from the Supplier. All payments made by the Authority to the Supplier are on an interim basis pending final resolution of an account with the Supplier in accordance with the terms of this Clause C1.

C1.16 The Supplier shall:

(a) add VAT to the Price at the prevailing rate as applicable and show the amount of VAT payable separately on all invoices as an extra charge. If the Supplier fails to show VAT on an invoice, the Authority is not, at any later date, liable to pay the Supplier any additional VAT;

(b) ensure that a provision is included in all Sub-Contracts which requires payment to be made of all sums due to Sub-Contractors within 30 days from the receipt of a valid invoice; and

(c) not suspend the Services unless the Supplier is entitled to terminate this Contract under Clause H2.3 for failure to pay undisputed sums of money.

C1.17 The Supplier indemnifies the Authority on a continuing basis against any liability, including any interest, penalties or costs incurred, which is levied, demanded or assessed on the Authority at any time in respect of the Supplier's failure to account for or to pay any VAT relating to payments made to the Supplier under this Contract. Any amounts due under this clause shall be paid by the Supplier to the Authority not less than five (5) Working Days before the date upon which the tax or other liability is payable by the Authority.

C1.18 The Authority shall:

(a) in addition to the Price and following receipt of a Valid Invoice, pay the Supplier a sum equal to the VAT chargeable on the value of the Services supplied in accordance with this Contract; and

(b) pay all sums due to the Supplier within 30 days of receipt of a Valid Invoice unless an alternative arrangement has been Approved.

C1.19 If the Authority fails to pay any undisputed invoices under this Contract, the Supplier may charge interest on the overdue amount at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from the due date up to the date of actual payment, whether before or after judgment.

C2 Recovery of Sums Due

C2.1 If under this Contract any sum of money is recoverable from or payable by the Supplier to the Authority (including any sum which the Supplier is liable to pay to the Authority in respect of any breach of this Contract), the Authority may unilaterally deduct that sum from any sum then due, or which at any later time may become due to the Supplier from the Authority under this Contract or under any other agreement with the Authority or the Crown.

C2.2 Any overpayment by either Party, whether of the Price or of VAT or otherwise, is a sum of money recoverable by the Party who made the overpayment from the Party in receipt of the overpayment.

C2.3 The Supplier shall make all payments due to the Authority without any deduction whether by way of set-off, counterclaim, discount, abatement or otherwise unless the Supplier has a valid court order requiring an amount equal to such deduction to be paid by the Authority to the Supplier.

C2.4 All payments due shall be made within a reasonable time unless otherwise specified in this Contract, in cleared funds, to such bank or building society account as the recipient Party may from time to time direct.

C3 NOT USED

C4 Establishment Service Cessation Deduction

C4.1 The Authority may at any point after the Services Commencement Date issue the Supplier with a notice instructing it to cease the provision of the Services at one or more Secure Establishment. Such notice will hereafter be referred to as an "**Establishment Service Cessation Notice**" or "**ESCN**".

C4.2 The Supplier will continue to provide the Services for the notice period stated in the ESCN (which shall be no less than three Months following the date of the ESCN). Thereafter the Supplier will no longer provide the Services to the relevant Secure Establishment for which the ESCN has been issued.

C4.3 With effect from expiry of the notice period set out in the ESCN the total Fixed Fees for the current and future Contract Years shall be reduced (pro rata, if necessary, in respect of the current Contract Year) by deducting the relevant Establishment Services Cessation Deduction allocated to the Secure Establishment that is the subject of the ESCN, as set out in the Fees Template. For the avoidance of doubt, such reduction shall not constitute a Change and therefore clause F4 shall not apply.

C4.4 Notwithstanding this, the reduction to the Fixed Fees shall be recorded in writing and signed by the duly authorised representative of each Party. As soon as reasonably practicable following such agreement, the Supplier shall provide to the Authority a revised Fees Template, to account for the reduction in the Fixed Fees in accordance with clause C4.3 for the Authority's approval.

C4.5 Within two calendar weeks of the date of the ESCN the Supplier will submit to the Authority its proposals for the demobilisation of the Services at the relevant Secure Establishment for which the ESCN has been issued. Such proposals will, among other things, include an exit plan (which shall be prepared on the same basis as the exit plan provided pursuant to Clause H9.6 (Exit Management)), record updates and the details and approach to case-load handover to ensure that cessation/handover of the Services are responsibly managed.

C4.6 The Authority shall review the Supplier's demobilisation proposals and will work with the Supplier to agree a demobilisation plan (which shall be implemented by the Supplier) which sets out how the Services at the relevant Secure Establishment for which the ESCN has been issued is to be demobilised throughout the duration of the notice period.

C4.7 The Supplier shall prepare and implement the demobilisation plan at no additional cost to the Authority.

D PROTECTION OF INFORMATION

D1 Authority Data

D1.1 The Supplier shall:

(a) not store, copy, disclose, or use the Authority Data except as necessary for the performance by the Supplier of its obligations under this Contract or as otherwise Approved;

(b) preserve the integrity of Authority Data and prevent the corruption or loss of Authority Data;

(c) not delete or remove any proprietary notices contained within or relating to the Authority Data;

(d) to the extent that Authority Data is held and/or processed by the Supplier, supply Authority Data to the Authority as requested by the Authority in the format specified in the Specification;

(e) perform secure back-ups of all Authority Data and ensure that up-to-date back-ups are stored securely off-site. The Supplier shall ensure that such back-ups are made available to the Authority immediately upon request;

(f) ensure that any system on which the Supplier holds any Authority Data, including back-up data, is a secure system that complies with the Security Policy Framework;

(g) identify, and disclose to the Authority on request those members of Staff with access to or who are involved in handling Authority Data;

(h) on request, give the Authority details of its policy for reporting, managing and recovering from information risk incidents, including losses of Personal Data, and its procedures for reducing risk;

(i) notify the Authority immediately and inform the Authority of the remedial action the Supplier proposes to take if it has reason to believe that Authority Data has or may become corrupted, lost or sufficiently degraded in any way for any reason; and

(j) comply with Schedule 6 (Security Requirements and Policy).

D1.2 If Authority Data is corrupted, lost or sufficiently degraded as a result of the Supplier's Default so as to be unusable, the Authority may:

(a) require the Supplier (at the Supplier's cost) to restore or procure the restoration of Authority Data and the Supplier shall do so promptly; and/or

(b) itself restore or procure the restoration of Authority Data and be repaid by the Supplier any reasonable costs incurred in doing so.

D2 Data Protection and Privacy

D2.1 The Parties acknowledge that for the purposes of the Data Protection Law, the nature of the Processing activity carried out by each of them in relation to their respective obligations under this Contract dictates the status of each Party. For the purposes of Processing Personal Data under this Contract, a Party may act as:

(a) "Controller" in respect of the other Party who is "Processor" (in which case, clauses D2.10 to D2.20 shall apply in addition to the General Obligations set out below);

(b) "joint Controller" with the other Party (in which case, clause D2.32 and the obligations set out in Annex 1 to Schedule 9 shall apply in addition to the General Obligations set out below);

(c) "independent Controller" of the Personal Data where the other Party is also "Controller" (in which case, clauses D2.21 to D2.31 shall apply in addition to the General Obligations set out below),

in respect of certain Personal Data Processed under or in connection with this Contract and shall specify in Schedule 9 *(Processing Personal Data)* which scenario shall apply in each situation.

General obligations that apply regardless of the relationship between the Parties ("General Obligations")

D2.2 Each Party shall at all times comply with its obligations under Data Protection Law.

D2.3 The Parties agree to take account of any guidance issued by the ICO and/or any relevant Regulatory Body. The Authority may on not less than thirty (30) Working Days' notice to the Supplier amend this Contract to ensure that it complies with any guidance issued by the ICO and/or any relevant Regulatory Body.

D2.4 Notwithstanding anything else in this clause D2 and subject to clauses H9.7 and H10, the Parties acknowledge and agree that the Authority shall not have access to CYP Personal Data , except where the Supplier is required to share limited CYP Personal Data with the Authority on a one-off basis for the purposes of Safeguarding or in accordance with clause D2.5 or to the extent that access to such CYP Personal Data is reasonably required in connection with an audit under clause F5 (Audit).

D2.5 On termination of this Contract, the Supplier shall, at the written direction of the Authority, transfer any Personal Data to any Replacement Supplier (or, if there is no Replacement Supplier, to the Authority) in accordance with the provisions in clause H9 (Exit Management), and delete any copies of such Personal Data upon termination of this Contract unless the Supplier is required by Law to retain copies the Personal Data.

D2.6 If financial penalties are imposed by the ICO on either the Authority or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

(a) if in the view of the ICO, the Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Authority, then the Authority shall be responsible for the payment of such Financial Penalties. In this case, the Authority will conduct an internal audit and engage, at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

(b) if in the view of the ICO, the Supplier is responsible for the Personal Data Breach, in that it is not a Personal Data Breach that the Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Authority and its auditors, on request and at the Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

(c) if no view as to responsibility is expressed by the ICO, then the Authority and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such dispute shall be referred to the dispute resolution procedure set out in clause I1 (Dispute Resolution).

D2.7 If either the Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction ("**Court**") by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

D2.8 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the "**Claim Losses**"):

(a) if the Authority is responsible for the relevant Personal Data Breach, then the Authority shall be responsible for the Claim Losses;

(b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

(c) if responsibility for the relevant Personal Data Breach is unclear, then the Authority and the Supplier shall be responsible for the Claim Losses equally.

D2.9 Nothing in either clause D2.7 or clause D2.8 shall preclude the Authority and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Authority.

Where one Party is Controller and the other Party its Processor

D2.10 Where a Party is Processing Personal Data as Processor under this Contract, the only Processing that it is authorised to do is listed in Schedule 9 by the Controller.

D2.11 The Processor shall Process Personal Data only on the Controller's instructions and shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Law.

D2.12 Where applicable, the Processor shall, at its own cost, provide all reasonable assistance to the Controller in the preparation of any DPIA prior to commencing any

Processing of Personal Data. Such assistance may, at the discretion of the Controller, include:

(a) a systematic description of the envisaged Processing and the purpose of the Processing;

(b) an assessment of the necessity and proportionality of the Processing in relation to the Services;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

D2.13 The Processor shall, in relation to any Personal Data Processed in connection with its obligations under this Contract:

(a) Process that Personal Data only in accordance with Schedule 9 unless the Processor is required to do otherwise by Law, in which case the Processor shall promptly notify the Controller before Processing the Personal Data unless prohibited by Law.

(b) ensure that it has in place Protective Measures which are appropriate to protect against a Data Loss Event which the Authority may reasonably reject. If the Authority reasonably rejects the Protective Measures put in place by the Processor, the Processor shall propose alternative Protective Measures to the satisfaction of the Authority. Any Protective Measures put in place by the Processor must take account of the nature of the Personal Data to be protected, the harm that might result from a Data Loss Event, the state of technological development and the cost of implementing any measures.

(c) ensure that:

i) Staff do not Process Personal Data except in accordance with this Contract and in particular Schedule 9;

ii) it takes all reasonable steps to ensure the reliability and integrity of any Staff who have access to the Personal Data and ensure that they:

A) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;

B) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by this Contract; and

C) have undergone adequate training in the use, care, protection and handling of Personal Data;

(d) not transfer Personal Data outside of the EU and the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

i) the destination country has been recognised as adequate by the Government in accordance with Article 45 of the UK GDPR (or s.74 of the DPA);

ii) if the destination country has not been recognised as adequate by the Government in accordance with Article 45 of the UK GDPR (or s.74 of the DPA), the following conditions are satisfied:

A) the Processor has appropriate safeguards in place in relation to the transfer (whether in accordance with UK GDPR Article 46 or s.75 of the DPA) as determined by the Controller; and

B) the Data Subject has enforceable rights and effective legal remedies;

iii) the Processor complies with its obligations under Data Protection Law by providing an adequate level of protection to any Personal Data that is transferred; and

iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data

D2.14 Subject to clause D2.15 below, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with this Contract, it:

i) receives a Data Subject Request (or purported Data Subject Request);

ii) receives a request to amend or erase any Personal Data;

iii) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Law;

iv) receives any communication from the ICO or any other regulatory authority in connection with Personal Data Processed under this Contract;

v) receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

vi) becomes aware of a Data Loss Event.

D2.15 The Processor's obligation to notify under clause D2.14 above shall include the provision of further information to the Controller in phases as details become available.

D2.16 Taking into account the nature of the Processing, the Processor shall provide the Controller with reasonable assistance in relation to either Party's obligations under Data Protection Law and any complaint, communication or request made under clause D2.14 above (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

(a) the Controller with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Law;

(c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Controller following any Data Loss Event; and

(e) assistance as requested by the Controller with respect to any request or communication from the ICO.

D2.17 Where necessary, the Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Clause D2 and the Data Protection Law.

D2.18 The Processor shall allow for audits of its Processing activity by the Authority or the Controller or the Controller's designated auditor. The Processor shall permit:

(a) the Controller, or a third-party auditor acting under the Controller's direction, to conduct data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this clause D2 and the Data Protection Law; and/or

(b) the Controller, or a third-party auditor acting under the Controller's direction, access to premises where the Personal Data is accessible or where it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to this Contract, and procedures, including premises under the control of any third party appointed by the Processor to assist in the provision of the Services.

The Controller may, in its sole discretion, require the Processor to provide evidence of the Processor's compliance with clause D2 in lieu of conducting such an audit, assessment or inspection.

D2.19 Before allowing any Sub-processor to Process any Personal Data related to this Contract, the Processor must:

(a) notify the Controller in writing of the intended Sub-processor and Processing:

(b) obtain the written consent of the Controller;

(c) enter into a written agreement with the Sub-processor which gives effect to the terms set out in these Clauses D2.10 to D2.20 such that they apply to the Sub-processor; and

(d) provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require;

provided that the Processor shall at all times remain fully liable for all acts or omissions of any of its Sub-processors.

D2.20 In relation to Processing for Law Enforcement Purposes, the Supplier shall:

(a) maintain logs for its automated Processing operations in respect of:

i) collection;

ii) alteration;

iii) consultation;

iv) disclosure (including transfers);

v) combination; and

vi) erasure.

(together the "**Logs**").

(b) ensure that:

i) the Logs of consultation make it possible to establish the justification for, and date and time of, the consultation; and as far as possible, the identity of the person who consulted the data;

ii) the Logs of disclosure make it possible to establish the justification for, and date and time of, the disclosure; and the identity of the recipients of the data; and

iii) the Logs are made available to the ICO on request

(c) use the Logs only to:

i) verify the lawfulness of Processing;

ii) assist with self-monitoring by the Authority or (as the case may be) the Supplier, including the conduct of internal disciplinary proceedings;

iii) ensure the integrity of Personal Data; and

iv) assist with criminal proceedings

(d) as far as possible, distinguish between Personal Data based on fact and Personal Data based on personal assessments; and

(e) where relevant and as far as possible, maintain a clear distinction between Personal Data relating to different categories of Data Subject, for example:

i) persons suspected of having committed or being about to commit a criminal offence;

ii) persons convicted of a criminal offence;

iii) persons who are or maybe victims of a criminal offence; and

iv) witnesses or other persons with information about offences.

Independent Controllers of Personal Data

D2.21 If and to the extent that each Party Processes Personal Data as an independent Controller, as set out in Schedule 9, each Party undertakes to comply with the applicable Data Protection Law in respect of their Processing of such Personal Data as independent Controller as set out below.

D2.22 Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Law and not do anything to cause the other Party to be in breach of it.

D2.23 Where a Party has provided Personal Data to the other Party under this clause D2 (or, in the case of the Supplier, where the Supplier has collected Personal Data as an independent Controller in performing its obligations under a Contract), the Party receiving (or, in the case of the Supplier, collecting) the Personal Data will, on request, provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

D2.24 The Parties shall be responsible for their own compliance with Articles 13 and 14 of the UK GDPR in respect of the Processing of Personal Data for the purposes of this Contract.

D2.25 The Parties shall only provide Personal Data to each other:

(a) to the extent necessary to perform their respective obligations under this Contract;

(b) in compliance with the Data Protection Law (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and

(c) in accordance with the details as set out in Schedule 9.

D2.26 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Law, including Article 32 of the UK GDPR.

D2.27 A Party Processing Personal Data for the purposes of this Contract shall maintain a record of its Processing activities in accordance with Article 30 of the UK GDPR and shall make the record available to the other Party upon reasonable request.

D2.28 Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Law in relation to the Personal Data provided to it by the other Party pursuant to this Contract ("**Request Recipient**"):

(a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

(b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Law.

D2.29 Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party (or, in the case of the Supplier, collected by the Supplier) pursuant to this Contract and shall:

(a) do all such things as reasonably necessary to mitigate, or (if appropriate) assist the other Party in mitigating, the effects of the Personal Data Breach;

(b) implement any measures necessary to restore the security of any compromised Personal Data;

(c) work with the other Party to make any required notifications to the ICO and affected Data Subjects in accordance with the Data Protection Law (including the timeframes set out therein); and

(d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

D2.30 Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under this Contract as specified in Schedule 9.

D2.31 Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under this Contract which is specified in Schedule 9.

Where the Parties are joint Controllers of Personal Data

D2.32 If and to the extent that the Parties are joint Controllers in respect of Processing Personal Data under this Contract, as set out in Schedule 9, the Parties shall implement paragraphs that are necessary to comply with the UK GDPR Article 26 based on the terms set out in Annex 1 to Schedule 9.

D3 Official Secrets Acts and Finance Act

D3.1 The Supplier shall comply with:

(a) the Official Secrets Acts 1911 to 1989; and

(b) section 182 of the Finance Act 1989.

D4 Confidential Information

D4.1 Except to the extent set out in clause D4 or if disclosure or publication is expressly allowed elsewhere in this Contract each Party shall treat all Confidential Information belonging to the other Party as confidential and shall not disclose any Confidential Information belonging to the other Party to any other person without the other Party's consent, except to such persons and to such extent as may be necessary for the performance of the Party's obligations under this Contract.

D4.2 The Supplier hereby gives its consent for the Authority to publish the whole Contract (but with any information which is Confidential Information belonging to the Authority redacted) including from time to time agreed changes to this Contract, to the general public.

D4.3 If required by the Authority, the Supplier shall ensure that Staff, professional advisors and consultants sign a non-disclosure agreement prior to commencing any work in connection with this Contract in a form approved by the Authority. The Supplier shall maintain a list of the non-disclosure agreements completed in accordance with this clause.

D4.4 If requested by the Authority, the Supplier shall give the Authority a copy of the list and, subsequently upon request by the Authority, copies of such of the listed non-disclosure agreements as required by the Authority. The Supplier shall ensure that Staff, professional advisors and consultants are aware of the Supplier's confidentiality obligations under this Contract.

D4.5 The Supplier may disclose the Authority's Confidential Information only to Staff who are directly involved in providing the Services and who need to know the information and shall ensure that such Staff are aware of and shall comply with these obligations as to confidentiality.

D4.6 The Supplier shall not, and shall procure that the Staff do not, use any of the Authority's Confidential Information received otherwise than for the purposes of this Contract.

D4.7 Clause D4.1 shall not apply to the extent that:

(a) such disclosure is a requirement of Law placed upon the Party making the disclosure, including any requirements for disclosure under the FOIA or the EIR;

(b) such information was in the possession of the Party making the disclosure without obligation of confidentiality prior to its disclosure by the information owner;

(c) such information was obtained from a third party without obligation of confidentiality;

(d) such information was already in the public domain at the time of disclosure otherwise than by a breach of this Contract; or

(e) it is independently developed without access to the other Party's Confidential Information.

D4.8 Nothing in clause D4.1 prevents the Authority disclosing any Confidential Information obtained from the Supplier:

(a) for the purpose of the examination and certification of the Authority's accounts;

(b) for the purpose of any examination pursuant to section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Authority has used its resources;

(c) to Parliament and Parliamentary committees;

(d) to any Crown Body or any Contracting Authority and the Supplier hereby acknowledges that all Government departments or Contracting Authorities receiving such Confidential Information may further disclose the Confidential Information to other Government departments or other Contracting Authorities on the basis that the information is confidential and is not to be disclosed to a third party which is not part of any Government department or any Contracting Authority; or

(e) to any consultant, contractor or other person engaged by the Authority

provided that in disclosing information under clauses D4.8 (d) and (e) the Authority discloses only the information which is necessary for the purpose concerned and requests that the information is treated in confidence and that a confidentiality undertaking is given where appropriate.

D4.9 Nothing in clauses D4.1 to D4.6 prevents either Party from using any techniques, ideas or Know-How gained during the performance of its obligations under this Contract in the course of its normal business, to the extent that this does not result in a disclosure of the other Party's Confidential Information or an infringement of the other Party's Intellectual Property Rights.

D4.10 The Authority shall use reasonable endeavours to ensure that any Government department, Contracting Authority, employee, third party or Sub-Contractor to whom the Supplier's Confidential Information is disclosed pursuant to clause D4.8 is made aware of the Authority's obligations of confidentiality.

D4.11 If the Supplier does not comply with clauses D4.1 to D4.8 the Authority may terminate this Contract immediately on notice.

D4.12 To ensure that no unauthorised person gains access to any Confidential Information or any data obtained in the supply of the Services, the Supplier shall maintain adequate security arrangements that meet the requirements of professional standards and best practice.

D4.13 The Supplier shall:

(a) immediately notify the Authority of any Breach of Security in relation to Confidential Information and all data obtained in the supply of the Services and will keep a record of such breaches;

(b) use best endeavours to recover such Confidential Information or data however it may be recorded;

(c) co-operate with the Authority in any investigation as a result of any breach of security in relation to Confidential Information or data; and

(d) at its own expense, alter any security systems at any time during the Term at the Authority's request if the Authority reasonably believes the Supplier has failed to comply with clause D4.12.

D5 Freedom of Information

D5.1 The Supplier acknowledges that the Authority is subject to the requirements of the FOIA and the EIR.

D5.2 The Supplier shall transfer to the Authority all Requests for Information that it receives as soon as practicable and in any event within 2 Working Days of receipt and shall:

(a) give the Authority a copy of all Information in its possession or control in the form that the Authority requires within 5 Working Days (or such other period as the Authority may specify) of the Authority's request;

(b) provide all necessary assistance as reasonably requested by the Authority to enable the Authority to comply with its obligations under the FOIA and EIR; and

(c) not respond directly to a Request for Information unless authorised to do so in writing by the Authority.

D5.3 The Authority shall determine in its absolute discretion and notwithstanding any other provision in this Contract or any other agreement whether the Commercially Sensitive Information and any other Information is exempt from disclosure in accordance with the FOIA and/or the EIR.

D6 Publicity, Media and Official Enquiries

D6.1 The Supplier shall not:

(a) make any press announcements or publicise this Contract or its contents in any way;

(b) use the Authority's name, brand or logo in any publicity, promotion, marketing or announcement of order; or

(c) use the name, brand or logo of any of the Authority's agencies or arms-length bodies in any publicity, promotion, marketing or announcement of orders

without Approval.

D6.2 Each Party acknowledges that nothing in this Contract either expressly or impliedly constitutes an endorsement of any products or services of the other Party (including the Services and the ICT Environment) and each Party shall not conduct itself in such a way as to imply or express any such approval or endorsement.

D6.3 The Supplier shall use reasonable endeavours to ensure that its Staff and professional advisors comply with clause D6.1.

E. INTELLECTUAL PROPERTY

E1 Intellectual Property Rights

E1.1 All Intellectual Property Rights in:

(a) the Results; and

(b) any guidance, specifications, reports, studies, instructions, toolkits, plans, data, drawings, databases, patents, patterns, models, designs or other material (save to the extent it comprises CYP Personal Data , subject to clauses H9.7 and H10) which is furnished to or made available to the Supplier by or on behalf of the Authority (together with the Results, the "**IP Materials**")

shall vest in the Authority (save for Copyright and Database Rights which shall vest in His Majesty the King) and the Supplier shall not, and shall ensure that the Staff shall not, use or disclose any IP Materials without Approval save to the extent necessary for performance by the Supplier of its obligations under this Contract.

E1.2 The Supplier hereby assigns:

(a) to the Authority, with full title guarantee, all Intellectual Property Rights (save for Copyright and Database Rights) which may subsist in the IP Materials. This assignment shall take effect on the date of this Contract or (in the case of rights arising after the date of this Contract) as a present assignment of future rights that will take effect immediately on the coming into existence of the Intellectual Property Rights produced by the Supplier; and

(b) to His Majesty the King, with full title guarantee, all Copyright and Database Rights which may subsist in the IP Materials,

and shall execute all documents and do all acts as are necessary to execute these assignments.

E1.3 The Supplier shall:

(a) waive or procure a waiver of any moral rights held by it or any third party in copyright material arising as a result of this Contract or the performance of its obligations under this Contract;

(b) ensure that the third-party owner of any Intellectual Property Rights that are or which may be used to perform the Services (other than CYP Personal Data , except to the extent that such access is required in connection with clauses H9.7 or H10 or in connection with an audit under clause F5 or for Safeguarding purposes) grants to the Authority a non-exclusive licence or, if itself a licensee

of those rights, shall grant to the Authority an authorised sub-licence, to use, reproduce, modify, develop and maintain the Intellectual Property Rights in the same. Such licence or sub-licence shall be non-exclusive, perpetual, royalty-free, worldwide and irrevocable and include the right for the Authority to sub-license, transfer, novate or assign to other Contracting Authorities, the Crown, the Replacement Supplier or to any other third-party supplying goods and/or services to the Authority ("**Indemnified Persons**");

(c) not infringe any Intellectual Property Rights of any third party in supplying the Services; and

(d) during and after the Term, indemnify and keep indemnified the Authority and Indemnified Persons from and against all actions, suits, claims, demands, losses, charges, damages, costs and expenses and other liabilities which the Authority and Indemnified Persons may suffer or incur as a result of or in connection with any breach of clause E1.3, except to the extent that any such claim results directly from:

i) items or materials based upon designs supplied by the Authority; or

ii) the use of data supplied by the Authority which is not required to be verified by the Supplier under any provision of this Contract.

E1.4 The Authority shall notify the Supplier in writing of any claim or demand brought against the Authority or Indemnified Person for infringement or alleged infringement of any Intellectual Property Right in materials supplied and/or licensed by the Supplier to the Authority.

E1.5 The Supplier shall at its own expense conduct all negotiations and any litigation arising in connection with any claim, demand or action by any third party for infringement or alleged infringement of any third party Intellectual Property Rights (whether by the Authority, the Supplier or Indemnified Person) arising from the performance of the Supplier's obligations under this Contract (**"Third Party IP Claim**"), provided that the Supplier shall at all times:

(a) consult the Authority on all material issues which arise during the conduct of such litigation and negotiations;

(b) take due and proper account of the interests of the Authority; and

(c) not settle or compromise any claim without Approval (not to be unreasonably withheld or delayed).

E1.6 The Authority shall, at the request of the Supplier, afford to the Supplier all reasonable assistance for the purpose of contesting any Third-Party IP Claim and the Supplier shall indemnify the Authority for all costs and expenses (including, but not limited to, legal costs and disbursements) incurred in doing so. The Supplier is not required to indemnify the Authority under this clause in relation to any costs and expenses to the extent that such arise directly from the matters referred to in clauses E1.3 (d) i) and ii).

E1.7 The Authority shall not, without the Supplier's consent, make any admissions which may be prejudicial to the defence or settlement of any Third-Party IP Claim.

E1.8 If any Third-Party IP Claim is made or in the reasonable opinion of the Supplier is likely to be made, the Supplier shall notify the Authority and any relevant Indemnified Person, at its own expense and subject to Approval (not to be unreasonably withheld or delayed), shall (without prejudice to the rights of the Authority under clauses E1.3 (b) and G2.1 (g)) use its best endeavours to:

(a) modify any or all of the Services without reducing the performance or functionality of the same, or substitute alternative services of equivalent performance and functionality, so as to avoid the infringement or the alleged infringement; or

(b) procure a licence to use the Intellectual Property Rights and supply the Services which are the subject of the alleged infringement, on terms which are acceptable to the Authority

and if the Supplier is unable to comply with clauses E1.8 (a) or (b) within 20 Working Days of receipt by the Authority of the Supplier's notification the Authority may terminate this Contract immediately by notice to the Supplier.

E1.9 The Supplier grants (or shall procure the grant of) to the Authority and, if requested by the Authority, to a Replacement Supplier, a royalty-free, perpetual, irrevocable, worldwide, non-exclusive licence (with a right to sub-license) to use: (a) any Intellectual Property Rights that the Supplier owns or has developed and/or (b) the CYP Data, and which in each case the Authority (or the Replacement Supplier) reasonably requires in order for the Authority to exercise its rights under, and receive the benefit of, this Contract (including, without limitation, the Services).

E1.10 The Authority grants (or shall procure the grant of) to the Supplier a royalty-free, perpetual, irrevocable, worldwide, non-exclusive licence (with a right to sub-license) to use the Intellectual Property Rights in the IP Materials as the Supplier reasonably requires in order for the Authority to exercise its obligations under this Contract.

F. CONTROL OF THE CONTRACT

F1 Contract Performance

F1.1 The Parties shall comply with their respective obligations, and shall be entitled to exercise their respective rights and remedies, as set out in Schedule 10 (Performance Mechanism).

F2 Remedies

F2.1 If the Authority reasonably believes the Supplier has committed a Material Breach it may, without prejudice to its rights under Clause H2 (Termination on Default), do any of the following:

(a) without terminating this Contract, itself supply or procure the supply of all or part of the Services until such time as the Supplier has demonstrated to the Authority's reasonable satisfaction that the Supplier will be able to supply the Services in accordance with the Specification;

(b) without terminating the whole of this Contract, terminate this Contract in respect of part of the Services only (whereupon a corresponding and proportionate

reduction in the Fixed Fees shall be made) and thereafter itself supply or procure a third party to supply such part of the Services;

(c) withhold or reduce payments to the Supplier in such amount as the Authority reasonably deems appropriate in each particular case; and/or

(d) terminate this Contract in accordance with Clause H2.

F2.2 Without prejudice to its right under Clause C2 (Recovery of Sums Due), the Authority may charge the Supplier for any costs reasonably incurred and any reasonable administration costs in respect of the supply of any part of the Services by the Authority or a third party to the extent that such costs exceed the payment which would otherwise have been payable to the Supplier for such part of the Services.

F2.3 If the Authority reasonably believes the Supplier has failed to supply all or any part of the Services in accordance with this Contract, professional or Good Industry Practice which could reasonably be expected of a competent and suitably qualified person, or any legislative or regulatory requirement, the Authority may give the Supplier notice specifying the way in which its performance falls short of the requirements of this Contract or is otherwise unsatisfactory.

F2.4 If the Supplier has been notified of a failure in accordance with clause F2.3 the Authority may:

(a) direct the Supplier to identify and remedy the failure within such time as may be specified by the Authority and to apply all such additional resources as are necessary to remedy that failure at no additional charge to the Authority within the specified timescale; and/or

(b) withhold or reduce payments to the Supplier in such amount as the Authority deems appropriate in each particular case until such failure has been remedied to the satisfaction of the Authority.

F2.5 If the Supplier has been notified of a failure in accordance with Clause F2.3, it shall:

(a) use all reasonable endeavours to immediately minimise the impact of such failure to the Authority and to prevent such failure from recurring; and

(b) immediately give the Authority such information as the Authority may request regarding what measures are being taken to comply with the obligations in Clause F2.5 and the progress of those measures until resolved to the satisfaction of the Authority.

F2.6 If, having been notified of any failure, the Supplier does not remedy it in accordance with Clause F2.5 in the time specified by the Authority, the Authority may treat the

continuing failure as a Material Breach and may terminate this Contract immediately on notice to the Supplier.

F3 Transfer and Sub-Contracting

F3.1 Except where both Clauses F3.9 and F3.10 apply, the Supplier shall not transfer, charge, assign, sub-contract or in any other way dispose of this Contract or any part of it without Approval. All such actions shall be evidenced in writing and shown to the Authority on request. Sub-contracting any part of this Contract does not relieve the Supplier of any of its obligations or duties under this Contract.

F3.2 The Supplier is responsible for the acts and/or omissions of its Sub-Contractors as though they are its own. If it is appropriate, the Supplier shall provide each Sub-Contractor with a copy of this Contract and obtain written confirmation from them that they will provide the Services fully in accordance with this Contract.

F3.3 The Supplier shall ensure that Sub-Contractors retain all records relating to the Services for at least six (6) years from the date of their creation and make them available to the Authority on request in accordance with Clause F5 (Audit). If any Sub-Contractor does not allow the Authority access to the records the Authority has no obligation to pay any claim or invoice made by the Supplier on the basis of such documents or work carried out by the Sub-Contractor.

F3.4 If the Authority has consented to the award of a Sub-Contract, the Supplier shall ensure that:

(a) the Sub-Contract contains:

i) a right for the Supplier to terminate if the Sub-Contractor does not comply with its legal obligations in connection with Data Protection Law, environmental, social or labour law; and

ii) obligations no less onerous on the Sub-Contractor than those on the Supplier under this Contract in respect of data protection in Clauses D1 and D2

(b) the Sub-Contractor includes a provision having the same effect as set out in this Clause F3.4 (a) in any Sub-Contract which it awards; and

(c) copies of each Sub-Contract are sent to the Authority immediately after their execution.

F3.5 Unless Approved otherwise, if the total value of this Contract over the Term is, or is likely to be, in excess of £5,000,000, the Supplier shall, in respect of Sub-Contract opportunities arising during the Term from or in connection with the provision of the Services:

(a) advertise on Contracts Finder those that have a value in excess of £25,000;

(b) within ninety (90) days of awarding a Sub-Contract, update the notice on Contracts Finder with details of the Sub-Contractor;

(c) monitor the number, type and value of the Sub-Contract opportunities placed on Contracts Finder and awarded during the Term;

(d) provide reports on the information in Clause F3.5(c) to the Authority in the format and frequency reasonably specified by the Authority;

(e) promote Contracts Finder to its suppliers and encourage them to register on Contracts Finder; and

(f) ensure that each advertisement placed pursuant to Clause F3.5(a) includes a full and detailed description of the Sub-Contract opportunity with each of the mandatory fields being completed on Contracts Finder.

F3.6 The Supplier shall, at its own cost, supply to the Authority by the end of April each year for the previous Financial Year:

(a) the total revenue received from the Authority pursuant to this Contract;

(b) the total value of all its Sub-Contracts;

(c) the total value of its Sub-Contracts with SMEs; and

(d) the total value of its Sub-Contracts with VCSEs.

F3.7 The Authority may from time to time change the format and the content of the information required pursuant to Clause F3.6.

F3.8 If the Authority believes there are:

(a) compulsory grounds for excluding a Sub-Contractor pursuant to regulation 57 of the Regulations, the Supplier shall replace or not appoint the Sub-Contractor; or

(b) non-compulsory grounds for excluding a Sub-Contractor pursuant to regulation 57 of the Regulations, the Authority may require the Supplier to replace or not appoint the Sub-Contractor and the Supplier shall comply with such requirement.

F3.9 Notwithstanding Clause F3.1, the Supplier may assign to a third party (the "**Assignee**") the right to receive payment of the Price or any part thereof due to the Supplier (including any interest which the Authority incurs under Clause C1 (Payment and VAT)). Any assignment under Clause F3.9 is subject to:

(a) reduction of any sums in respect of which the Authority exercises its right of recovery under Clause C2 (Recovery of Sums Due);

(b) all related rights of the Authority under this Contract in relation to the recovery of sums due but unpaid; and

(c) the Authority receiving notification under both Clauses F3.10 and F3.11.

F3.10 If the Supplier assigns the right to receive the Price under Clause F3.9, the Supplier or the Assignee shall notify the Authority in writing of the assignment and the date upon which the assignment becomes effective.

F3.11 The Supplier shall ensure that the Assignee notifies the Authority of the Assignee's contact information and bank account details to which the Authority can make payment.

F3.12 Clause C1 continues to apply in all other respects after the assignment and shall not be amended without Approval.

F3.13 Subject to Clause F3.14, the Authority may assign, novate or otherwise dispose of its rights and obligations under this Contract or any part thereof to:

(a) any Contracting Authority;

(b) any other body established or authorised by the Crown or under statute in order substantially to perform any of the functions that had previously been performed by the Authority; or

(c) any private sector body which substantially performs the functions of the Authority

provided that any such assignment, novation or other disposal shall not increase the burden of the Supplier's obligations under this Contract.

F3.14 Any change in the legal status of the Authority such that it ceases to be a Contracting Authority shall not, subject to Clause F3.15, affect the validity of this Contract and this Contract shall bind and inure to the benefit of any successor body to the Authority.

F3.15 If the rights and obligations under this Contract are assigned, novated or otherwise disposed of pursuant to Clause F3.13 to a body which is not a Contracting Authority or if there is a change in the legal status of the Authority such that it ceases to be a Contracting Authority (in the remainder of this clause both such bodies being referred to as the **"Transferee"**):

(a) the rights of termination of the Authority in Clauses H1 and H2 are available to the Supplier in respect of the Transferee; and

(b) the Transferee shall only be able to assign, novate or otherwise dispose of its rights and obligations under this Contract or any part thereof with the prior consent in writing of the Supplier.

F3.16 The Authority may disclose to any Transferee any Confidential Information of the Supplier which relates to the performance of the Supplier's obligations under this Contract. In such circumstances the Authority shall authorise the Transferee to use such Confidential Information only for purposes relating to the performance of the Supplier's obligations under this Contract and for no other purpose and shall take all reasonable steps to ensure that the Transferee gives a confidentiality undertaking in relation to such Confidential Information.

F3.17 Each Party shall at its own cost and expense carry out, or use all reasonable endeavours to ensure the carrying out of, whatever further actions (including the execution of further documents) the other Party reasonably requires from time to time for the purpose of giving that other Party the full benefit of this Contract.

F4 Change

F4.1 After the Commencement Date, either Party may request a Change subject to the terms of this clause F4.

F4.2 Either Party may request a Change by notifying the other Party in writing of the Change by completing the Change Request Form set out in Schedule 3. Any additional charges associated with a Change shall be proportionate to the Fixed Fees set out in the Fees Template and shall be in accordance with any costing principles set out in the Fees Template. The Party requesting the Change shall give the other Party sufficient information and time to assess the extent and effect of the requested Change. If the receiving Party accepts the Change it shall confirm it in writing to the other Party.

F4.3 If the Supplier is unable to accept a Change requested by the Authority or if the Parties are unable to agree a change to the Price, the Authority may:

(a) allow the Supplier to fulfil its obligations under this Contract without the Change; or

(b) terminate this Contract immediately except where the Supplier has already delivered all or part of the Services or where the Supplier can show evidence of substantial work being carried out to fulfil the requirements of the Specification; and in such case the Parties shall attempt to agree upon a resolution to the matter. If a resolution cannot be reached, the matter shall be dealt with under the Dispute Resolution procedure detailed in clause I2 (Dispute Resolution).

F4.4 A Change takes effect only when it is recorded in a CCN validly executed by both Parties.

F4.5 The Supplier is deemed to warrant and represent that the CCN has been executed by a duly authorised representative of the Supplier in addition to the warranties and representations set out in clause G2.

F4.6 Clauses F4.4 and F4.5 may be varied in an emergency if it is not practicable to obtain the Authorised Representative's approval within the time necessary to make the Change in order to address the emergency. In an emergency, Changes may be approved by a different representative of the Authority. However, the Authorised Representative may review such a Change and require a CCN to be entered into on a retrospective basis which may itself vary the emergency Change.

F5 Audit

F5.1 The Supplier shall:

(a) keep and maintain for 6 years after the end of the Term, or as long a period as may be agreed between the Parties, full and accurate records of its compliance with, and discharge of its obligations under this Contract including the Services supplied under it, all expenditure reimbursed by the Authority, and all payments made by the Authority;

(b) on request afford the Authority or the Authority's representatives such access to those records and processes as may be requested by the Authority in connection with this Contract; and

(c) make available to the Authority, free of charge, whenever requested, copies of audit reports obtained by the Supplier in relation to the Services.

F5.2 The Authority, acting by itself or through its duly authorised representatives and/or the National Audit Office, may, during the Term and for a period of 18 Months thereafter, assess compliance by the Supplier of the Supplier's obligations under this Contract, including to:

(a) verify the accuracy of the Price and any other amounts payable by the Authority under this Contract;

(b) verify the Open Book Data;

(c) verify the Supplier's compliance with this Contract and applicable Law;

(d) identify or investigate actual or suspected fraud, impropriety or accounting mistakes or any breach or threatened Breach of Security and in these circumstances the Authority has no obligation to inform the Supplier of the purpose or objective of its investigations;

(e) identify or investigate any circumstances which may impact upon the financial stability of the Supplier and/or any guarantor or their ability to perform the Services;

(f) obtain such information as is necessary to fulfil the Authority's obligations to supply information for parliamentary, ministerial, judicial or administrative purposes;

(g) carry out the Authority's internal and statutory audits and to prepare, examine and/or certify the Authority's annual and interim reports and accounts;

(h) enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Authority has used its resources;

(i) verify the accuracy and completeness of any management information or reports delivered or required by this Contract;

(j) review the Supplier's compliance with the Policies and Standards; and/or

(k) review the integrity, confidentiality and security of the Authority Data

and the Supplier (and its agents) shall permit access free of charge during normal business hours on reasonable notice to all such documents (including computerised documents and data) and other information as the Authority (or those acting on its behalf) may reasonably require for the purposes of conducting such an audit.

F5.3 The Supplier (and its agents) shall permit the Comptroller and Auditor General (and his appointed representatives) access free of charge during normal business hours on reasonable notice to all such documents (including computerised documents and data) and other information as the Comptroller and Auditor General may reasonably require for the purposes of conducting a financial audit of the Authority and for carrying out examinations into the economy, efficiency and effectiveness with which the

Authority has used its resources. The Supplier shall provide such explanations as are reasonably required for these purposes.

F5.4 The Authority shall during each audit comply with those security, sites, systems and facilities operating procedures of the Supplier that the Authority deems reasonable and use its reasonable endeavours to ensure that the conduct of each audit does not unreasonably disrupt the Supplier or delay the provision of the Services. The Authority shall endeavour to (but is not obliged to) provide at least fifteen (15) Working Days' notice of its intention to conduct an audit.

F5.5 The Parties bear their own respective costs and expenses incurred in respect of compliance with their obligations under clause F5, unless the audit identifies a material Default by the Supplier in which case the Supplier shall reimburse the Authority for all the Authority's reasonable costs incurred in connection with the audit.

G. LIABILITIES

G1 Liability, Indemnity and Insurance

G1.1 Neither Party limits its liability for:

(a) death or personal injury caused by its negligence;

(b) fraud or fraudulent misrepresentation;

(c) any breach of any obligations implied by section 12 of the Sale of Goods Act 1979 or section 2 of the Supply of Goods and Services Act 1982;

(d) any breach of clauses D1 (Authority Data), D2 (Data Protection and Privacy) or D4 (Confidential Information) or Schedule 6 (Information Security & Assurance) or Schedule 8 (Statutory Obligations and Corporate Social Responsibility); or

(e) any liability under clauses B10.5 (Employment), C1.17 (VAT), E1.3 (Intellectual; Property Rights), G3.2 (Tax Compliance) and H8.4 (Retendering and Handover); or

(f) any liability to the extent it cannot be limited or excluded by Law.

G1.2 Subject to clauses G1.3 and G1.5, the Supplier indemnifies the Authority fully against all claims, proceedings, demands, charges, actions, damages, costs, breach of statutory duty, expenses and any other liabilities which may arise out of the supply, or the late or purported supply, of the Services or the performance or non-performance by the Supplier of its obligations under this Contract or the presence of the Supplier or any Staff on the Premises, including in respect of any death or personal injury, loss of or damage to property, financial loss arising from any advice given or omitted to be given by the Supplier, or any other loss which is caused directly by any act or omission of the Supplier.

G1.3 Subject to clause G1.1 the Supplier's aggregate liability in respect of:

(a) loss of or damage to the Authority Premises, Authority Equipment or other property or assets of the Authority (including technical infrastructure, assets or equipment but excluding any loss or damage to the Authority's Data or any other

data) that is caused by Defaults of the Supplier occurring in each and any Contract Year shall in no event exceed £20,000,000;

(b) all other Losses incurred by the Authority under or in connection with this Contract as a result of Defaults by the Supplier shall in no event exceed:

i) in relation to Defaults occurring in the first Contract Year, an amount equal to 150% of the Estimated Year 1 Price;

ii) in relation to Defaults occurring during any subsequent Contract Year, an amount equal to 150% of the Fixed Fees paid and/or due to be paid to the Supplier under this Contract in this Contract Year immediately preceding the occurrence of the Default; and

ii) in relation to Defaults occurring after the end of the Term, an amount equal to 150% of the Fixed Fees paid and/or due to be paid to the Supplier in the 12 month period immediately prior to the last day of the Term.

G1.4 Subject to clause G1.1 the Authority's aggregate liability in respect of this Contract does not exceed the Price payable in the previous calendar year of this Contract.

G1.5 The Supplier is not responsible for any injury, loss, damage, cost or expense if and to the extent that it is caused by the negligence or wilful misconduct of the Authority or by breach by the Authority of its obligations under this Contract.

G1.6 The Authority may recover from the Supplier the following losses incurred by the Authority to the extent they arise as a result of a Default by the Supplier:

(a) any additional operational and/or administrative costs and expenses incurred by the Authority, including costs relating to time spent by or on behalf of the Authority in dealing with the consequences of the Default;

(b) any wasted expenditure or charges;

(c) the additional costs of procuring a Replacement Supplier for the remainder of the Term and or replacement deliverables which shall include any incremental costs associated with the Replacement Supplier and/or replacement deliverables above those which would have been payable under this Contract;

(d) any compensation or interest paid to a third party by the Authority; and

(e) any fine or penalty incurred by the Authority pursuant to Law and any costs incurred by the Authority in defending any proceedings which result in such fine or penalty.

G1.7 Subject to clauses G1.1 and G1.6, neither Party is liable to the other for any:

(a) loss of profits, turnover, business opportunities or damage to goodwill; or

(b) indirect, special or consequential loss.

G1.8 Unless otherwise specified by the Authority, the Supplier shall, with effect from the Commencement Date for such period as necessary to enable the Supplier to comply with its obligations herein, take out and maintain with a reputable insurance company

a policy or policies of insurance providing an adequate level of cover in respect of all risks which may be incurred by the Supplier, arising out of the Supplier's performance of its obligations under this Contract including:

(a) professional indemnity insurance in the sum of not less than £2,000,000 in respect of any one claim or series of connected claims for any advice given by the Supplier to the Authority;

(b) public liability insurance in the sum of not less than £20,000,000 in respect of any one claim or series of connected claims for any advice given by the Supplier to the Authority;

(c) employer's liability insurance with cover (for a single event or a series of related events and in the aggregate) of not less than five million pounds (£5,000,000);

(d) product liability insurance in the sum of not less than £20,000,000 in respect of any one claim or series of connected claims.

Such insurance policies shall be maintained for the duration of the Term and for a minimum of 6 years following the end of the Term.

G1.9 The Supplier shall give the Authority, on request, copies of all insurance policies referred to in this clause or a broker's verification of insurance to demonstrate that the appropriate cover is in place, together with receipts or other evidence of payment of the latest premiums due under those policies.

G1.10 If the Supplier does not have and maintain the insurances required by this Contract, the Authority may make alternative arrangements to protect its interests and may recover the costs of such arrangements from the Supplier.

G1.11 The provisions of any insurance or the amount of cover shall not relieve the Supplier of any liabilities under this Contract.

G1.12 The Supplier shall not take any action or fail to take any reasonable action, or (to the extent that it is reasonably within its power) permit anything to occur in relation to the Supplier, which would entitle any insurer to refuse to pay any claim under any insurance policy in which the Supplier is an insured, a co-insured or additional insured person.

G2 Warranties and Representations

G2.1 The Supplier warrants and represents on the Commencement Date and for the Term that:

(a) it has full capacity and authority and all necessary consents to enter into and perform this Contract and that this Contract is executed by a duly authorised representative of the Supplier;

(b) in entering this Contract, it has not committed any fraud;

(c) all written statements and representations in any written submissions made by the Supplier as part of the procurement process, including without limitation its response to the selection questionnaire and invitation to tender, its Tender (including the Supplier Proposal) and any other documents submitted by the

Supplier to the Authority remains true, accurate and not misleading, except to the extent that such statements and representations have been superseded or varied by this Contract or to the extent that the Supplier has otherwise disclosed to the Authority in writing prior to the date of this Contract, and in addition that it will advise the Authority of any fact, matter or circumstance of which it may become aware which would render such information, statements or representations to be false or misleading;

(d) no claim is being asserted and no litigation, arbitration or administrative proceeding is in progress or, to the best of its knowledge and belief, pending or threatened against it or any of its assets which will or might have an adverse effect on its ability to perform its obligations under this Contract;

(e) it is not subject to any contractual obligation, compliance with which is likely to have a material adverse effect on its ability to perform its obligations under this Contract;

(f) no proceedings or other steps have been taken and not discharged (or, to the best of its knowledge, are threatened) for the winding up of the Supplier or for its dissolution or for the appointment of a receiver, administrative receiver, liquidator, manager, administrator or similar officer in relation to any of the Supplier's assets or revenue;

(g) it owns, or has obtained or is able to obtain valid licences for, all Intellectual Property Rights that are necessary for the performance of its obligations under this Contract;

(h) any person engaged by the Supplier shall be engaged on terms which do not entitle them to any Intellectual Property Right in any IP Materials;

(i) in the 3 years (or period of existence if the Supplier has not been in existence for 3 years) prior to the date of this Contract:

i) it has conducted all financial accounting and reporting activities in compliance in all material respects with the generally accepted accounting principles that apply to it in any country where it files accounts;

ii) it has been in full compliance with all applicable securities and tax laws and regulations in the jurisdiction in which it is established; and

iii) it has not done or omitted to do anything which could have a material adverse effect on its assets, financial condition or position as an ongoing business concern or its ability to fulfil its obligations under this Contract;

(j) it has and will continue to hold all necessary (if any) regulatory approvals from the Regulatory Bodies necessary to perform its obligations under this Contract; and

(k) it has notified the Authority in writing of any Occasions of Tax Non-Compliance and any litigation in which it is involved that is in connection with any Occasion of Tax Non-Compliance.

G2.2 The Supplier confirms that in entering into this Contract it is not relying on any statements, warranties or representations given or made (whether negligently or innocently or whether express or implied), or any acts or omissions by or on behalf of

the Authority in connection with the subject matter of this Contract except those expressly set out in this Contract and the Supplier hereby waives and releases the Authority in respect thereof absolutely.

G3 Tax Compliance

G3.1 If, during the Term, an Occasion of Tax Non-Compliance occurs, the Supplier shall:

(a) notify the Authority in writing of such fact within 5 Working Days of its occurrence; and

(b) promptly give the Authority:

i) details of the steps it is taking to address the Occasion of Tax Non-Compliance and to prevent the same from recurring, together with any mitigating factors it considers relevant; and

ii) such other information in relation to the Occasion of Tax Non-Compliance as the Authority may reasonably require.

G3.2 If the Supplier or any Staff are liable to be taxed in the UK or to pay NICs in respect of consideration received under this Contract, the Supplier shall:

(a) at all times comply with ITEPA and all other statutes and regulations relating to income tax, and SSCBA and all other statutes and regulations relating to NICs, in respect of that consideration; and

(b) indemnify the Authority against any income tax, NICs and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made in connection with the provision of the Services by the Supplier or any Staff.

H. DEFAULT, DISRUPTION AND TERMINATION

H1 Insolvency and Change of Control

H1.1 The Authority may terminate this Contract with immediate effect by notice and without compensation to the Supplier if the Supplier is a company and in respect of the Supplier:

(a) a proposal is made for a voluntary arrangement within Part I of the Insolvency Act 1986 or of any other composition scheme or arrangement with, or assignment for the benefit of, its creditors;

(b) a shareholders' meeting is convened for the purpose of considering a resolution that it be wound up or a resolution for its winding-up is passed (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation);

(c) a petition is presented for its winding up (which is not dismissed within 14 days of its service) or an application is made for the appointment of a provisional liquidator;

(d) a receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets;

(e) an application order is made either for the appointment of an administrator or for an administration order, an administrator is appointed, or notice of intention to appoint an administrator is given;

(f) it is or becomes insolvent within the meaning of section 123 of the Insolvency Act 1986; or

(g) any event similar to those listed in H1.1 (a)-(f) occurs under the law of any other jurisdiction.

H1.2 The Authority may terminate this Contract with immediate effect by notice and without compensation to the Supplier if the Supplier is an individual and:

(a) an application for an interim order is made pursuant to sections 252-253 of the Insolvency Act 1986 or a proposal is made for any composition scheme or arrangement with, or assignment for the benefit of, the Supplier's creditors;

(b) a petition is presented and not dismissed within 14 days or order made for the Supplier's bankruptcy;

(c) a receiver, or similar officer is appointed over the whole or any part of the Supplier's assets or a person becomes entitled to appoint a receiver, or similar officer over the whole or any part of his assets;

(d) he is unable to pay his debts or has no reasonable prospect of doing so, in either case within the meaning of section 268 of the Insolvency Act 1986;

(e) a creditor or encumbrancer attaches or takes possession of, or a distress, execution, sequestration or other such process is levied or enforced on or sued against, the whole or any part of the Supplier's assets and such attachment or process is not discharged within 14 days;

(f) he dies or is adjudged incapable of managing his affairs within the meaning of section 2 of the Mental Capacity Act 2005;

(g) he suspends or ceases, or threatens to suspend or cease, to carry on all or a substantial part of his business; or

(h) any event similar to those listed in clauses H1.2(a) to (g) occurs under the law of any other jurisdiction.

H1.3 The Supplier shall notify the Authority immediately following a merger, take-over, change of control, change of name or status including where the Supplier undergoes a change of control within the meaning of section 1124 of the Corporation Tax Act 2010 (**"Change of Control"**). The Authority may terminate this Contract with immediate effect by notice and without compensation to the Supplier within 6 Months of:

(a) being notified that a Change of Control has occurred; or

(b) where no notification has been made, the date that the Authority becomes aware of the Change of Control,

but is not permitted to terminate where Approval was granted prior to the Change of Control.

H1.4 The Authority may terminate this Contract with immediate effect by notice and without compensation to the Supplier if the Supplier is a partnership and:

(a) a proposal is made for a voluntary arrangement within Article 4 of the Insolvent Partnerships Order 1994 or a proposal is made for any other composition, scheme or arrangement with, or assignment for the benefit of, its creditors; or

(b) a petition is presented for its winding up or for the making of any administration order, or an application is made for the appointment of a provisional liquidator; or

(c) a receiver, or similar officer is appointed over the whole or any part of its assets; or

(d) the partnership is deemed unable to pay its debts within the meaning of section 222 or 223 of the Insolvency Act 1986 as applied and modified by the Insolvent Partnerships Order 1994; or

(e) any of the following occurs in relation to any of its partners:

(i) an application for an interim order is made pursuant to sections 252-253 of the Insolvency Act 1986 or a proposal is made for any composition scheme or arrangement with, or assignment for the benefit of, his creditors;

(ii) a petition is presented for his bankruptcy; or

(iii) a receiver, or similar officer is appointed over the whole or any part of his assets;

(f) any event similar to those listed in clauses H1.4 (a) to (e) occurs under the law of any other jurisdiction.

H1.5 The Authority may terminate this Contract with immediate effect by notice and without compensation to the Supplier if the Supplier is a limited liability partnership and:

(a) a proposal is made for a voluntary arrangement within Part I of the Insolvency Act 1986 or a proposal is made for any other composition, scheme or arrangement with, or assignment for the benefit of, its creditors;

(b) an application is made either for the appointment of an administrator or for an administration order, an administrator is appointed, or notice of intention to appoint an administrator is given within Part II of the Insolvency Act 1986;

(c) any step is taken with a view to it being determined that it be wound up (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation) within Part IV of the Insolvency Act 1986;

(d) a petition is presented for its winding up (which is not dismissed within 14 days of its service) or an application is made for the appointment of a provisional liquidator within Part IV of the Insolvency Act 1986;

(e) a receiver, or similar officer is appointed over the whole or any part of its assets;

(f) it is or becomes unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986; or

(g) any event similar to those listed in clauses H1.5 (a) to (f) occurs under the law of any other jurisdiction.

H1.6 References to the Insolvency Act 1986 in clause H1.5 (a) are references to that Act as applied under the Limited Liability Partnerships Act 2000 subordinate legislation.

H2 Default

H2.1 The Authority may terminate this Contract with immediate effect by notice if the Supplier commits a Default and:

(a) the Supplier has not remedied the Default to the satisfaction of the Authority within 20 Working Days or such other period as may be specified by the Authority, after issue of a notice specifying the Default and requesting it to be remedied;

(b) the Default is not, in the opinion of the Authority, capable of remedy; or

(c) the Default is a Material Breach.

H2.2 If, through any Default of the Supplier, data transmitted or processed in connection with this Contract is either lost or sufficiently degraded as to be unusable, the Supplier is liable for the cost of reconstitution of that data and shall reimburse the Authority in respect of any charge levied for its transmission and any other costs charged in connection with such Default.

H2.3 If the Authority fails to pay the Supplier undisputed sums of money when due, the Supplier shall give notice to the Authority of its failure to pay. If the Authority fails to pay such undisputed sums within 90 Working Days of the date of such notice, the Supplier may terminate this Contract with immediate effect, save that such right of termination shall not apply where the failure to pay is due to the Authority exercising its rights under clause C2.1 or to a Force Majeure Event.

H3 Termination on Notice

H3.1 The Authority may terminate this Contract at any time by giving no less than 90 days' notice to the Supplier.

H3A Termination for Prolonged Force Majeure Events

H3A.1 If a Force Majeure Event continues for a period of ninety (90) Working Days or more from the date upon which the Affected Party serves notice on the other Party of its occurrence, either Party may by twenty (20) Working Days' notice to the other Party:

(a) terminate any Services affected by the Force Majeure Event;

(b) if substantially all of the Affected Party's obligations have been affected by the Force Majeure Event, terminate this Contract as a whole;

and this Contract (or the part of this Contract related to the affected Services) shall be terminated.

H3A.2 The costs of termination incurred by the Parties shall lie where they fall if a Party terminates or partially terminates this Contract for a continuing Force Majeure Event pursuant to Clause H3A.1.

H4 Other Termination Grounds

H4.1 The Authority may terminate this Contract if:

(a) this Contract has been subject to a substantial modification which requires a new procurement procedure pursuant to regulation 72(9) of the Regulations;

(b) the Supplier was, at the time this Contract was awarded, in one of the situations specified in regulation 57(1) of the Regulations, including as a result of the application of regulation 57(2), and should therefore have been excluded from the procurement procedure which resulted in its award of this Contract;

(c) this Contract should not have been awarded to the Supplier in view of a serious infringement of the obligations under the Public Contracts Regulations 2015 (as amended); or

(d) the Supplier has not, in performing the Services, complied with its legal obligations in respect of environmental, social or labour law.

H5 Consequences of Expiry or Termination

H5.1 If the Authority terminates this Contract under clause H2 and makes other arrangements for the supply of the Services the Authority may recover from the Supplier the cost reasonably incurred of making those other arrangements and any additional expenditure incurred by the Authority throughout the remainder of the Term.

H5.2 If this Contract is terminated under clause H2 the Authority shall make no further payments to the Supplier (for Services supplied by the Supplier prior to termination and in accordance with this Contract but where the payment has yet to be made by the Authority), until the Authority has established the final cost of making the other arrangements envisaged under this clause H5.

H5.3 If the Authority terminates this Contract by exercising the Break Option or under clauses H3 or H4 the Authority shall make no further payments to the Supplier except for Services supplied by the Supplier prior to termination and in accordance with this Contract but where the payment has yet to be made by the Authority.

H5.4 Save as otherwise expressly provided in this Contract:

(a) termination or expiry of this Contract shall be without prejudice to any rights, remedies or obligations accrued under this Contract prior to termination or

expiration and nothing in this Contract prejudices the right of either Party to recover any amount outstanding at such termination or expiry; and

(b) termination of this Contract does not affect the continuing rights, remedies or obligations of the Authority or the Supplier under clauses C2 (Payment and VAT), C3 (Recovery of Sums Due), D2 (Data Protection and Privacy), D3 (Official Secrets Acts and Finance Act), D4 (Confidential Information), D5 (Freedom of Information), E1 (Intellectual Property Rights), F5 (Audit), G1 (Liability, Indemnity and Insurance), H5 (Consequences of Expiry or Termination), H7 (Recovery), H8 (Retendering and Handover), H9 (Exit Management), H10 (Knowledge Retention), I6 (Remedies Cumulative), I12 (Governing Law and Jurisdiction) and paragraph 9 of Schedule 8.

H6 Disruption and Business Continuity Plan

H6.1 The Supplier shall take reasonable care to ensure that in the performance of its obligations under this Contract it does not disrupt the operations of the Authority, its employees or any other contractor employed by the Authority.

H6.2 The Supplier shall immediately inform the Authority of any actual or potential industrial action, whether such action be by its own employees or others, which affects or might affect its ability at any time to perform its obligations under this Contract.

H6.3 If there is industrial action by Staff, the Supplier shall seek Approval for its proposals to continue to perform its obligations under this Contract.

H6.4 If the Supplier's proposals referred to in clause H6.3 are considered insufficient or unacceptable by the Authority acting reasonably, this Contract may be terminated with immediate effect by the Authority.

H6.5 If the Supplier is unable to deliver the Services owing to disruption of the Authority's normal business, the Supplier may request a reasonable allowance of time, and, in addition, the Authority will reimburse any additional expense reasonably incurred by the Supplier as a direct result of such disruption.

H6.6 The Parties shall comply with their respective obligation in respect of the Business Continuity Plan in accordance with Schedule 11 (Business Continuity Plan).

H7 Recovery

H7.1 On termination of this Contract for any reason, the Supplier shall at its cost:

(a) immediately return to the Authority all Confidential Information, Personal Data and IP Materials in its possession or in the possession or under the control of any permitted suppliers or Sub-Contractors, which was obtained or produced in the course of providing the Services;

(b) immediately deliver to the Authority all Authority Equipment (including materials, documents, information and access keys) provided to the Supplier in good working order;

(c) immediately vacate any Authority Premises occupied by the Supplier;

(d) assist and co-operate with the Authority to ensure an orderly transition of the provision of the Services to the Replacement Supplier and/or the completion of any work in progress; and

(e) promptly provide all information concerning the provision of the Services which may reasonably be requested by the Authority for the purposes of adequately understanding the manner in which the Services have been provided and/or for the purpose of allowing the Authority and/or the Replacement Supplier to conduct due diligence.

H7.2 If the Supplier does not comply with clauses H7.1 (a) and (b), the Authority may recover possession thereof and the Supplier grants a licence to the Authority or its appointed agents to enter (for the purposes of such recovery) any premises of the Supplier or its suppliers or Sub-Contractors where any such items may be held.

H8 Retendering and Handover

H8.1 Within 21 days of being requested by the Authority, the Supplier shall provide, and thereafter keep updated, in a fully indexed and catalogued format, all the information necessary to enable the Authority to issue tender documents for the future provision of the Services.

H8.2 The Authority shall take all necessary precautions to ensure that the information referred to in clause H8.1 is given only to potential providers who have qualified to tender for the future provision of the Services.

H8.3 The Authority shall require that all potential providers treat the information in confidence; that they do not communicate it except to such persons within their organisation and to such extent as may be necessary for the purpose of preparing a response to an invitation to tender issued by the Authority; and that they shall not use it for any other purpose.

H8.4 The Supplier indemnifies the Authority against any claim made against the Authority at any time by any person in respect of any liability incurred by the Authority arising from any deficiency or inaccuracy in information which the Supplier is required to provide under clause H8.1.

H8.5 The Supplier shall allow access to the Premises in the presence of an authorised representative, to any person representing any potential provider whom the Authority has selected to tender for the future provision of the Services.

H8.6 If access is required to the Supplier's Premises for the purposes of clause H8.5, the Authority shall give the Supplier 7 days' notice of a proposed visit together with a list showing the names of all persons who will be visiting. Their attendance shall be subject to compliance with the Supplier's security procedures, subject to such compliance not being in conflict with the objectives of the visit.

H8.7 The Supplier shall co-operate fully with the Authority during any handover at the end of this Contract. This co-operation includes allowing full access to, and providing copies of, all documents, reports, summaries and any other information necessary in order to achieve an effective transition without disruption to routine operational requirements.

H8.8 Within 10 Working Days of being requested by the Authority, the Supplier shall transfer to the Authority, or any person designated by the Authority, free of charge, all computerised filing, recording, documentation, planning and drawing held on software and utilised in the provision of the Services. The transfer shall be made in a fully indexed and catalogued disk format, to operate on a proprietary software package identical to that used by the Authority.

H9 Exit Management

H9.1 On termination of this Contract the Supplier shall render reasonable assistance to the Authority to the extent necessary to effect an orderly assumption by a Replacement Supplier in accordance with the procedure set out in clauses H9.2 to H9.5 and any Exit Plan.

H9.2 If the Authority requires a continuation of all or any of the Services on expiry or termination of this Contract, either by performing them itself or by engaging a third party to perform them, the Supplier shall co-operate fully with the Authority and any such third party and shall take all reasonable steps to ensure the timely and effective transfer of the Services without disruption to routine operational requirements.

H9.3 The following commercial approach shall apply to the transfer of the Services:

(a) if the Supplier does not have to use resources in addition to those normally used to deliver the Services prior to termination or expiry, there shall be no change to the Price; or

(b) if the Supplier reasonably incurs additional costs, the Parties shall agree a Change to the Price based on and in line with the Supplier's rates either set out in Schedule 2 or forming the basis for the Price.

H9.4 When requested to do so by the Authority, the Supplier shall deliver to the Authority details of all licences for software used in the provision of the Services including the software licence agreements.

H9.5 Within one Month of receiving the software licence information described in clause H9.4, the Authority shall notify the Supplier of the licences it wishes to be transferred and the Supplier shall provide for the approval of the Authority a plan for licence transfer.

H9.6 The Supplier shall provide a draft exit plan for Approval in accordance with Schedule 15 (Exit Plan).

H9.7 On termination of this Contract the Supplier shall, at the written direction of the Authority, and subject to Clause H9.7A:

(a) transfer any CYP Data (including CYP Personal Data and Live Cases), as applicable (and as directed by the Authority) to the Replacement Supplier (or, if there is no Replacement Supplier, to the Authority);

(b) share Live Cases with the Replacement Supplier (or, if there is no Replacement Supplier, with the Authority) in compliance with the Data Protection Law, and the Supplier shall provide written confirmation to the Authority of this;

(c) delete any copies of Personal Data that it holds unless the Supplier is required by Law to retain copies of such Personal Data;

(d) return any Personal Data as applicable to the Authority; and/or

(e) take any other actions regarding Personal Data as instructed by the Authority.

H9.7A The Supplier and the Authority acknowledge that the Supplier is required, and shall therefore be entitled, to retain CYP Personal Data that forms part of Closed Cases. The Supplier shall retain such data until the relevant Child or Young Person's 75th birthday and shall ensure that such data (together with any copies of such data) is securely deleted on that date.

H10 Knowledge Retention

The Supplier shall co-operate fully with the Authority in order to enable an efficient and detailed knowledge transfer from the Supplier to the Authority on the completion or earlier termination of this Contract and in addition, to minimise any disruption to routine operational requirements. To facilitate this transfer, the Supplier shall provide the Authority free of charge with full access to its Staff, and in addition, copies of all documents, reports, summaries and any other information requested by the Authority. The Supplier shall comply with the Authority's request for information no later than fifteen (15) Working Days from the date that that request was made.

H11 Supplier Relief

H11.1 Notwithstanding any other provision of this Contract, if the Supplier has failed to comply with its obligations under this Contract, achieve a Milestone by its Milestone Date or provide the Services in accordance with the CDIs (each a "**Supplier Non-Performance**") and can demonstrate that the Supplier Non-Performance would not have occurred but for an Authority Cause, then (subject to the Supplier fulfilling its obligations in this Clause H11, including Clause H11.4) the Authority may at its option:

(a) without prejudice to clause H11.3, grant the Supplier a reasonable extension of time in order to allow the Supplier to rectify the Supplier Non-Performance to the Authority's reasonable satisfaction; and/or

(b) where the Supplier Non-Performance constitutes a failure of any CDIs, temporarily suspend the application of such CDI(s), including any liability of the Supplier to deduct the Financial Remedy, for the duration that the Supplier Non-Performance continues,

in each case, to the extent that the Supplier can demonstrate that the CDI failure was caused by the Authority Cause.

H11.2 In order to claim any of the rights and/or relief referred to in Clause H11.1, the Supplier shall as soon as reasonably practicable (and in any event within ten (10) Working

Days) after becoming aware that an Authority Cause has caused, or is reasonably likely to cause, a Supplier Non-Performance, give the Authority notice (a "**Relief Notice**") setting out details of:

(a) the Supplier Non-Performance;

(b) the Authority Cause and its effect, or likely effect, on the Supplier's ability to meet its obligations under this Contract; and

(c) any steps which the Authority can take to eliminate or mitigate the consequences and impact of such Authority Cause.

H11.3 Following the receipt of a Relief Notice, the Authority shall as soon as reasonably practicable consider the nature of the Supplier Non-Performance and the alleged Authority Cause and whether it agrees with the Supplier's assessment set out in the Relief Notice as to the effect of the relevant Authority Cause and its entitlement to relief, consulting with the Supplier where necessary.

H11.4 The Supplier shall use all reasonable endeavours to eliminate or mitigate the consequences and impact of an Authority Cause (which may, where appropriate, include implementing the Business Continuity Plan), including any Losses that the Supplier may incur and, if relevant, the duration and consequences of any delay or anticipated delay to the achievement of any Milestone(s). The Supplier shall, notwithstanding the Authority Cause, continue to provide the Services to the extent possible, which may include providing the Services via alternative means (such as face-to-face or via the internet or telephone, depending on the nature and the impact of the Authority Cause).

H11.5 If a Dispute arises as to whether a Supplier Non-Performance would not have occurred but for an Authority Cause or the nature and/or extent of the relief and/or compensation claimed by the Supplier, either Party may refer the dispute to the dispute resolution procedure set out in Clause I1. Pending the resolution of the dispute, both Parties shall continue to resolve the causes of, and mitigate the effects of, the Supplier Non-Performance.

H11.6 Any Change that is required to the Mobilisation Plan or to the Price pursuant to this Clause H11 shall be implemented in accordance with the change control procedure at Clause F4.

I GENERAL

I1 Dispute Resolution

I1.1 The Parties shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with this Contract within 20 Working Days of either Party notifying the other of the dispute and such efforts shall involve the escalation of the dispute to the finance director of the Supplier and the commercial director of the Authority.

I1.2 Nothing in this dispute resolution procedure prevents the Parties seeking from any court of competent jurisdiction an interim order restraining the other Party from doing any act or compelling the other Party to do any act.

I1.3 If the dispute cannot be resolved by the Parties pursuant to clause I1.1 either Party may refer it to mediation pursuant to the procedure set out in clause I1.5.

I1.4 The obligations of the Parties under this Contract shall not cease, or be suspended or delayed by the reference of a dispute to mediation (or arbitration) and the Supplier and the Staff shall comply fully with the requirements of this Contract at all times.

I1.5 The procedure for mediation and consequential provisions relating to mediation are as follows:

(a) a neutral adviser or mediator (the **"Mediator"**) shall be chosen by agreement of the Parties or, if they are unable to agree upon a Mediator within 10 Working Days after a request by one Party to the other or if the Mediator agreed upon is unable or unwilling to act, either Party shall within 10 Working Days from the date of the proposal to appoint a Mediator or within 10 Working Days of notice to either Party that he is unable or unwilling to act, apply to the Centre for Effective Dispute Resolution to appoint a Mediator;

(b) the Parties shall within 10 Working Days of the appointment of the Mediator meet with him in order to agree a programme for the exchange of all relevant information and the structure to be adopted for negotiations. If appropriate, the Parties may at any stage seek assistance from the Centre for Effective Dispute Resolution to provide guidance on a suitable procedure;

(c) unless otherwise agreed, all negotiations connected with the dispute and any settlement agreement relating to it shall be conducted in confidence and without prejudice to the rights of the Parties in any future proceedings;

(d) if the Parties reach agreement on the resolution of the dispute, the agreement shall be recorded in writing and shall be binding on the Parties once it is signed by their duly authorised representatives;

(e) failing agreement, either of the Parties may invite the Mediator to provide a non-binding but informative written opinion. Such an opinion shall be provided on a without prejudice basis and shall not be used in evidence in any proceedings relating to this Contract without the prior written consent of both Parties; and

(f) if the Parties fail to reach agreement within 60 Working Days of the Mediator being appointed, or such longer period as may be agreed by the Parties, then any dispute or difference between them may be referred to the Courts unless the dispute is referred to arbitration pursuant to the procedures set out in clause I1.6.

I1.6 Subject to clause I1.2, the Parties shall not start court proceedings until the procedures set out in clauses I1.1 and I1.3 have been completed save that:

(a) the Authority may at any time before court proceedings are commenced, serve a notice on the Supplier requiring the dispute to be referred to and resolved by arbitration in accordance with clause I1.7;

(b) if the Supplier intends to commence court proceedings, it shall serve notice on the Authority of its intentions and the Authority has 21 days following receipt of such notice to serve a reply on the Supplier requiring the dispute to be referred to and resolved by arbitration in accordance with clause I1.7; and

(c) the Supplier may request by notice to the Authority that any dispute be referred and resolved by arbitration in accordance with clause I1.7, to which the Authority may consent as it sees fit.

I1.7 If any arbitration proceedings are commenced pursuant to clause I1.6:

(a) the arbitration is governed by the Arbitration Act 1996 and the Authority shall give a notice of arbitration to the Supplier (the "**Arbitration Notice**") stating:

(i) that the dispute is referred to arbitration; and

(ii) providing details of the issues to be resolved;

(b) the London Court of International Arbitration (**"LCIA"**) procedural rules in force at the date that the dispute was referred to arbitration in accordance with I1.7 (b) shall be applied and are deemed to be incorporated by reference to this Contract and the decision of the arbitrator is binding on the Parties in the absence of any material failure to comply with such rules;

(c) the tribunal shall consist of a sole arbitrator to be agreed by the Parties;

(d) if the Parties fail to agree the appointment of the arbitrator within 10 days of the Arbitration Notice being issued by the Authority under clause I1.7 (a) or if the person appointed is unable or unwilling to act, the arbitrator shall be appointed by the LCIA;

(e) the arbitration proceedings shall take place in London and in the English language; and

(f) the arbitration proceedings shall be governed by, and interpreted in accordance with, English Law.

I2 Force Majeure

I2.1 Subject to this clause I2, a Party may claim relief under this clause I2 from liability for failure to meet its obligations under this Contract for as long as and only to the extent that the performance of those obligations is directly affected by a Force Majeure Event. Any failure or delay by the Supplier in performing its obligations under this Contract which results from a failure or delay by an agent, Sub-Contractor or supplier is regarded as due to a Force Majeure Event only if that agent, Sub-Contractor or supplier is itself impeded by a Force Majeure Event from complying with an obligation to the Supplier.

I2.2 The Affected Party shall as soon as reasonably practicable issue a Force Majeure Notice, which shall include details of the Force Majeure Event, its effect on the obligations of the Affected Party and any action the Affected Party proposes to take to mitigate its effect.

I2.3 If the Supplier is the Affected Party, it is not entitled to claim relief under this clause I2 to the extent that consequences of the relevant Force Majeure Event:

(a) are capable of being mitigated by any of the Services, but the Supplier has failed to do so; and/or

(b) should have been foreseen and prevented or avoided by a prudent provider of services similar to the Services, operating to the standards required by this Contract.

I2.4 Subject to clause I2.5, as soon as practicable after the Affected Party issues the Force Majeure Notice, and at regular intervals thereafter, the Parties shall consult in good faith and use reasonable endeavours to agree any steps to be taken and an appropriate timetable in which those steps should be taken, to enable continued provision of the Services affected by the Force Majeure Event.

I2.5 The Parties shall at all times following the occurrence of a Force Majeure Event and during its subsistence use their respective reasonable endeavours to prevent and mitigate the effects of the Force Majeure Event. Where the Supplier is the Affected Party, it shall take all steps in accordance with Good Industry Practice to overcome or minimise the consequences of the Force Majeure Event.

I2.6 Subject to clause H3A (Termination for Prolonged Force Majeure Events), If, as a result of a Force Majeure Event:

(a) an Affected Party fails to perform its obligations in accordance with this Contract, then during the continuance of the Force Majeure Event:

i) the other Party is not entitled to exercise its rights to terminate this Contract in whole or in part as a result of such failure pursuant to clause H2.1 or H2.3; and

ii) neither Party is liable for any Default arising as a result of such failure;

(b) the Supplier fails to perform its obligations in accordance with this Contract it is entitled to receive payment of the Price (or a proportional payment of it) only to the extent that the Services (or part of the Services) continue to be performed in accordance with this Contract during the occurrence of the Force Majeure Event.

I2.7 The Affected Party shall notify the other Party as soon as practicable after the Force Majeure Event ceases or no longer causes the Affected Party to be unable to comply with its obligations under this Contract.

I2.8 Relief from liability for the Affected Party under this clause I2 ends as soon as the Force Majeure Event no longer causes the Affected Party to be unable to comply with its obligations under this Contract and is not dependent on the serving of a notice under clause I2.7.

I3 Notices and Communications

I3.1 Subject to clause I3.3, where this Contract states that a notice or communication between the Parties must be “written” or “in writing” it is not valid unless it is made by letter (sent by hand, first class post, recorded delivery or special delivery) or by email or by communication via Bravo.

I3.2 If it is not returned as undelivered a notice served in:

(a) a letter is deemed to have been received 2 Working Days after the day it was sent; and

(b) an email is deemed to have been received 4 hours after the time it was sent provided it was sent on a Working Day,

or when the other Party acknowledges receipt, whichever is the earlier.

I3.3 Notices pursuant to clauses I1, I2 or I7 or to terminate this Contract or any part of the Services are valid only if served in a letter by hand, recorded delivery or special delivery.

I3.4 Notices shall be sent to the addresses set out below or at such other address as the relevant Party may give notice to the other Party for the purpose of service of notices under this Contract:

(a) For the Authority:

Contact Name: [redacted]Associate Commercial Specialist – MOJ, Commercial and Contract Management Directorate;

Address: 102 Petty France, London SW1H 9AJ, and

Email: [redacted]

(b) For the Supplier:

Contact Name: [redacted]

Address: Barnardo's: Your Rights Your Voice, Rockford House, Low lane, Horsforth, LS18 5QW; and

Email: [redacted]

I4 Conflicts of Interest

I4.1 The Supplier shall take appropriate steps to ensure that neither the Supplier nor any Staff is placed in a position where, in the reasonable opinion of the Authority, there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the Supplier and the duties owed to the Authority under this Contract. The Supplier will notify the Authority immediately giving full particulars of any such conflict of interest which may arise.

I4.2 The Authority may terminate this Contract immediately by notice and/or take or require the Supplier to take such other steps it deems necessary if, in the Authority's reasonable opinion, there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the Supplier and the duties owed to the Authority under this Contract. The actions of the Authority pursuant to this clause I4 shall not prejudice or affect any right of action or remedy which shall have accrued or shall thereafter accrue to the Authority.

I5 Rights of Third Parties

I5.1 Clause E1.3 and paragraph 2.5 of Schedule 19 (Staff Transfers) confer benefits on persons named in them (together "**Third Party Provisions**" and each person a "**Third Party Beneficiary**") other than the Parties and are intended to be enforceable by

Third Party Beneficiaries by virtue of the Contracts (Rights of Third Parties) Act 1999 ("**CRTPA**").

I5.2 Subject to clause I5.1, a person who is not a Party has no right under the CRTPA to enforce this Contract but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to the CRTPA and does not apply to the Crown.

I5.3 No Third-Party Beneficiary may enforce or take steps to enforce any Third-Party Provision without Approval.

I5.4 Any amendments to this Contract may be made by the Parties without the consent of any Third-Party Beneficiary.

I6 Remedies Cumulative

Except as expressly provided in this Contract all remedies available to either Party for breach of this Contract are cumulative and may be exercised concurrently or separately, and the exercise of any one remedy are not an election of such remedy to the exclusion of other remedies.

I7 Waiver

I7.1 The failure of either Party to insist upon strict performance of any provision of this Contract, or the failure of either Party to exercise, or any delay in exercising, any right or remedy do not constitute a waiver of that right or remedy and do not cause a diminution of the obligations established by this Contract.

I7.2 No waiver is effective unless it is expressly stated to be a waiver and communicated to the other Party in writing in accordance with clause I3 (Notices and Communications).

I7.3 A waiver of any right or remedy arising from a breach of this Contract does not constitute a waiver of any right or remedy arising from any other or subsequent breach of this Contract.

I8 Severability

If any part of this Contract which is not of a fundamental nature is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such part shall be severed and the remainder of this Contract shall continue in full effect as if this Contract had been executed with the invalid, illegal or unenforceable part eliminated.

I9 Entire Agreement

The Contract constitutes the entire agreement between the Parties in respect of the matters dealt with therein. Neither Party has been given, nor entered into this Contract in reliance on, any warranty, statement, promise or representation other than those expressly set out in this Contract. The Contract supersedes all prior negotiations between the Parties and all representations and undertakings made by one Party to the other, whether written or oral, except that this clause shall not exclude liability in respect of any fraudulent misrepresentation.

I10 Change in Law

I10.1 The Supplier is neither relieved of its obligations to supply the Services in accordance with the terms and conditions of this Contract nor entitled to an increase in the Price as the result of:

(a) a General Change in Law; or

(b) a Specific Change in Law where the effect of that Specific Change in Law on the Services is reasonably foreseeable at the Commencement Date.

I10.2 If a Specific Change in Law occurs or will occur during the Term (other than as referred to in clause I10.1(b)), the Supplier shall:

(a) notify the Authority as soon as reasonably practicable of the likely effects of that change, including whether any:

(i) Change is required to the Services, the Price or this Contract; and

(ii) relief from compliance with the Supplier's obligations is required; and

(b) provide the Authority with evidence:

(i) that the Supplier has minimised any increase in costs or maximised any reduction in costs, including in respect of the costs of its Sub-Contractors; and

(ii) as to how the Specific Change in Law has affected the cost of providing the Services.

I10.3 Any variation in the Price or relief from the Supplier's obligations resulting from a Specific Change in Law (other than as referred to in clause I10.1(b)) shall be implemented in accordance with clause F4.

I11 Counterparts

The Contract may be executed in counterparts, each of which when executed and delivered constitute an original but all counterparts together constitute one and the same instrument.

I12 Governing Law and Jurisdiction

Subject to clause I1 (Dispute Resolution) this Contract, including any matters arising out of or in connection with it, are governed by and interpreted in accordance with English Law and are subject to the jurisdiction of the Courts of England and Wales. The submission to such jurisdiction does not limit the right of the Authority to take proceedings against the Supplier in any other court of competent jurisdiction, and the taking of proceedings in any other court of competent jurisdiction does not preclude the taking of proceedings in any other jurisdiction whether concurrently or not.

SCHEDULE 1 – SPECIFICATION

SCHEDULE 1: AUTHORITY'S REQUIREMENTS (SERVICE SPECIFICATION)

EXECUTIVE SUMMARY

Statement and purpose of the requirement

1. This specification sets out the services required to provide Independent Children's Rights and Advocacy Services in youth custody: for all Children and Young People held in Secure Training Centres (STCs) and under-18 Young Offender Institutions (YOIs).

2. Independent Children's Rights and Advocacy Services are commissioned to offer an independent voice for Children and Young People empowering them to make sure that their views and wishes are heard and that their rights are respected. Advocacy supports Children and Young People to represent their views to decision-makers, and to help them to resolve their issues relating to their welfare, care and treatment whilst in, as well as navigate, youth custody and the wider youth justice system.

3. Providing advocacy services supports statutory responsibilities and duties placed upon the YCS and MoJ, including protecting children's and human rights. Advocacy provision also very clearly aligns with the evidence base for working with Children and Young People, supporting pro-social identities, active engagement, and in promoting their voices and views.

Secure Establishments

4. The Services shall be provided to all Children and Young People remanded and sentenced to custody in STC and (under-18) YOI accommodation throughout England and Wales, as set out in Schedule 7 (Secure Establishments).

5. These Services are not delivered to Children and Young People given custodial sentences and placed into Secure Children's Homes (SCHs) or Secure Schools, as the legal and statutory framework for these premises already requires the provision of advocacy.

6. Where relevant, the Supplier is expected to work with advocates at SCHs or Secure Schools on behalf of Children and Young People who transfer to/ from STCs/ YOIs.

7. The Supplier will provide a flexible service that can readily respond to the changing needs of Children and Young People in Youth Custody. This Schedule will be subject to ongoing review and development by both the Authority and the Supplier to take note of emerging best practice and changes in approach. Any change to this Schedule agreed by the Parties shall be made in accordance with clause F4 (Change).

8. Advocacy Services in Youth Custody must adhere to the National Standards for the Provision of Children's Advocacy Services and the Advocacy Standards and Outcomes Framework for Children and Young People from Wales.

Legislative and Statutory Requirements

9. All services working with Children and Young People in the youth justice system must adhere to Standards for children in the youth justice system - GOV.UK (www.gov.uk) and be aware of and work to Healthcare standards for Children and Young People in secure settings.

10. In adherence to these Standards and in promoting the rights of Children and Young People, the Services will follow and adhere to the broad legal frameworks of the United Nations Convention on the Rights of the Child (UNCRC) and the European Convention on Human Rights (ECHR).1

11. Other principal statutory requirements for Children and Young People in Youth Custody in England and/ or Wales – within which this Specification is set, and that are given in Schedule 8 (Statutory Obligations and Corporate Social Responsibility) of this Contract, and that the Supplier is obliged to ensure are applied to these Services – are contained in the following (and updated as amended):

    - Prison Service Instruction (PSI): Care and Management of Young People (Revised 2020)
    - Searching Policy Framework - GOV.UK (www.gov.uk)
    - Minimising and Managing Use of Separation and Isolation in the Children and Young People Secure Estate, 2020
    - The Young Offender Institution Rules 2000
    - The Secure Training Centre Rules 1998
    - Crime and Disorder Act 1998
    - Working together to safeguard children, 2018
    - Wales Safeguarding Procedures
    - Safeguarding Vulnerable Groups Act 2006
    - Health and Care Act 2022
    - The Data Protection Act 2018
    - Children and Families Act 2014
    - Social Services and Well-being (Wales) Act 2014
    - Welsh Language (Wales) Measure 2011
    - Equality Act 2010
    - Mental Health Act 2007
    - Children Act 2004
    - Care Standards Act 2000

12. The Advocacy Services for Children and Young People in the secure estate will be fully independent of organisations running Secure Establishments – Advocates also provide for the function of "independent persons" within STCs. [2] The categories of persons who are not to be considered 'independent' are set out in the Definitions of Independent Visitors (Children) Regulations 1991 and include:

    - where the person appointed is connected with any organisation responsible for accommodating the Young Person by virtue of being:
        - a member of that organisation;

[1] Human Rights: The UK's international human rights obligations - GOV.UK (www.gov.uk)
[2] See Rule 44 of the STC Rules

- a patron or trustee of that organisation;
- an employee of that organisation, whether paid or not; or
- a spouse or co-habiting partner of any such person.

Principles of Advocacy

13. The Supplier must deliver Advocacy Services that enshrine the National Standards, which means that:

- Advocacy is led by Children and Young Peoples' wishes and views, and the whole model of the Services shall be informed by such.
- The Services support Children and Young People so that they are able to understand and exercise their rights. It empowers Children and Young People to represent themselves and ensure their rights are respected and their views and wishes are heard.
- All Children and Young People can access the Services equally, without discrimination. The Services are designed to work with the individual and protected characteristics of each Child or Young Person, including being respectful of their culture and background.
- Advocacy Services operate independently of Secure Establishments, and respect Children and Young People's privacy and confidentiality.
- Each Child and Young Person receives a high-quality service that is timely in supporting their wishes, needs and dignity throughout their custodial experience.
- Safeguarding and promoting the welfare of Children and Young People will be at the heart of the Supplier's ethos and culture.

Structuring these Requirements

14. The specification applies to the Services commissioned by the Authority for Children and Young People in STCs and YOIs – as detailed in the Executive Summary of this Schedule 1. This Schedule covers the required services to be delivered by the Supplier under this Contract, constructed under the Sections and Headings given on p6.

15. This Specification is outcome focussed and outlines the minimum operational service requirements for Advocacy Services, following the structure as set out below:

Outcomes
Outcomes for Children and Young People that this area of Supplier services will contribute to achieving.
Service Requirements
The minimum requirements of the Supplier in contributing to the outcomes for Children and Young People, as set out in the "Outcomes" section above, being achieved. The Supplier has the flexibility and is encouraged to deliver innovative solutions that will achieve, but may go over and above, the minimum requirements specified in this section.

CHILDREN AND YOUNG PEOPLE'S ADVOCACY SERVICES IN YOUTH CUSTODY

Section	Heading
1	Overview of Advocacy Services Delivery
2	Safeguarding and Protecting Children and Young People
3	Staffing Leadership, Management and Workforce
4	Working with Secure Establishments and Other Services for Children and Young People
5	Contract Management, Service Assurance and Improvement
6	Optional Services
7	Social Value

Section 1 : Overview of Advocacy Services Delivery

Outcomes
• Children and Young People know that an independent Advocacy Service is available to them and can easily access this when they need it and that this includes being able to access support outside of service hours onsite at Secure Establishments and receiving a response within a specified timescale to any messages they leave. • Children and Young People know that Advocacy Services work exclusively for them and that independent Advocacy Services can help them. • Children and Young People understand and are confident that Advocacy Services respect their privacy and confidentiality. • All Children and Young People are aware of and can access Advocacy Services without fear of discrimination. • Advocacy Services respect Children and Young Peoples' cultural and religious needs and are delivered/ available in the language of their choice – *including where Children and Young People speak Welsh.* • Children and Young People accessing Advocacy Services are supported and empowered to have their views and wishes heard and their rights respected. *Including Children and Young People:* – *wishing to make a representation or complaint, or to seek specialist or legal advice;* – *wishing to make a representation or complaint concerning the Advocacy Services and of the ways available to do this;* – *being able to exercise their right to change an Advocate/s representing them.* • Children and Young People accessing Advocacy Services are informed about their rights. • Children and Young People are supported, prepared and are more confident when presenting their views directly to decision makers.
Service Requirements
1.1 Publicising the Services to Children and Young People 1.1.1 The Supplier shall ensure the Services are effectively publicised on each residential unit and wing in use for Children and Young People within each Secure Establishment, including healthcare units, enhanced support units, and care and separation units. The Supplier shall also effectively publicise Advocacy Services in other areas that Children and Young People regularly use – such as visit halls/ centres, gymnasium and sports areas, and in reception. This can include but is not limited to: a) photographs, where possible of the Supplier's Staff for the Secure Establishment; b) details of how the Supplier's Staff can be contacted, including the helpline number and digital access details;

c) details of when the Supplier's Staff will undertake Unit Visits at the Secure Establishment/ residential unit/ wing;

d) providing comprehensive, co-produced and customised information packs to Children and Young People on induction to the Secure Establishment;

e) (secure) post boxes are not required but should be available as part of a solution that includes written physical referrals.

1.1.2 Children and Young People must be able to easily understand and access information provided to publicise the Advocacy Services, physically, digitally and via any helpline, including being available in language/s the Child or Young Person understands.

1.1.3 The Supplier shall engage with Children and Young People to consider how effective the publicity methods are and in order to co-produce developments and improvements to these.

1.2 Children and Young People are aware of the Service

1.2.1 The Supplier's Staff shall visit every Child and Young Person newly admitted at the Secure Establishment within 72 hours of their arrival, to make them aware of the role of Advocacy Services, that these are available to help and support them, and of their right to access Advocates.

1.2.1.A This visit must be made in-person / face-to-face by the Supplier's Staff – other methods (such as a video-call) are only acceptable in exceptional, contingent or emergency operating conditions, as approved or instructed on a case-by-case basis by the Authority at its discretion.

1.2.1.B Newly admitted to the Secure Establishment is where any Child or Young Person arrives at the relevant Secure Establishment from the community or bail (via court or, occasionally, direct from the Police), or from another Secure Establishment. Children and Young People are not newly admitted to the Secure Establishment where they are returning to the Establishment from a day appearance in court, or moving between units within the STC/ YOI. Exemptions from this may apply in specific cases (as approved or determined on a case-by-case basis by the Authority at its discretion) where, for example, a newly admitted Child or Young Person leaves the Secure Establishment within 72hrs of their arrival.

1.2.2 Each Child or Young Person must, following this visit, have information available to them that explains the various ways they can contact the Advocacy Services. This can include, but is not limited to:

a) digital access through Child and Young Person personal digital devices (in-bedroom technology);

b) a telephone helpline – when not serviced by the Supplier's Staff, an answerphone service must be in place covering out of office hours, and any periods of absence e.g. sickness/special circumstances;

c) secure post boxes located on residential units where Children and Young People can submit applications for visit requests; and

d) an appropriate route for applications for advocacy support via Secure Establishment (and other) staff.

1.2.3 Digital and physical contact methods will be accessed by identified Supplier personnel regularly to ensure a swift response/ contact with the Child or Young Person to any messages left.

1.3 Children and Young People are introduced to the Service

1.3.1 Inductions will be used to alleviate any concerns the Child or Young Person has and should be used as an opportunity to explore the Child or Young Person's personal circumstances and identify the potential support that the Child or Young Person may need.

1.3.2 Inductions should always be carried out in a confidential environment. The first day after reception to the Secure Establishment is deemed as "day one". The number of new admissions include Children or Young People transferred into the YOI/ STC from another Secure Establishment. The agreed procedure for Inductions at each Secure Establishment will be captured in the Local Protocols at Schedule 12 (Local Protocols).

1.3.3 The Supplier shall ensure management oversite and quality assurance of the provision of Services, and that Children and Young People are provided with appropriate Children's Rights and Advocacy Service information at the point of admission. This quality assurance will include visits to Children and Young People who have recently been admitted to the Secure Establishment to ensure that they have received information on the Advocacy Service and on Children and Young People's human rights on admission and induction.

1.3.4 The Supplier's Staff shall then, separate to the visits required at paragraph 1.2.1, conduct a meeting with each Child and Young Person as part of their Induction to the Secure Establishment – within 7 Calendar Days of their arrival – to:

a) Introduce themselves and provide the Child or Young Person with details of the Service, who the different members of the advocacy team at that Secure Establishment are and what their roles are.

b) Provide the Child or Young Person with details regarding what the Services can and cannot offer and explain the principles of the Services – including that Services are independent, confidential, and work exclusively on behalf of the Child or Young Person.

Children and Young People may find it helpful to be provided with examples of the types of issues or concerns that Advocates can help with, and the support available.

c) Explain the various ways to contact the Supplier and make a referral to the Advocacy Services.

d) Provide details of when the Supplier's Staff undertake Unit Visits at the Secure Establishment.

e) Explain how Children and Young People can make a complaint about the Services.

1.3.5 The Supplier's Staff can tailor each Induction meeting according to the Child or Young Person's previous experience (including of custody) and their personal circumstances, as long as this still achieves the outcomes for this Section 1.

1.3.6 The Supplier will provide Children and Young People with – or make available to them – (within 7 calendar days of their arrival) a range of comprehensive information on the Services, which will be appropriate to the needs of the Child or Young Person – having been co-produced with Children and Young People and designed with consideration of their age, development, and experiences.

1.3.7 This information will be accessible, in a language/s, format/s and style/s that Children and Young People can understand – including for Children and Young People who consider themselves/ are considered to have a physical or learning disability. Information must be made available in Welsh for Children and Young People who are from Wales.

1.3.8 The availability and accessibility of the information must be effective at reminding Children and Young People of the availability of Advocacy Services throughout their time in youth custody. The information should be updated alongside and to reflect any fundamental service changes agreed with the Secure Establishment or Authority

1.4 Children's and Young People's Rights Awareness Session

1.4.1 The Supplier is required to deliver the minimum agreed Children and Young People's Rights Awareness Sessions at each Secure Establishment.

1.4.2 A Children's and Young People's Rights Awareness Session is defined as being:

a) A session for each Child and Young Person as part of their Induction to the Secure Establishment – i.e. within the first 14 calendar days of their time in custody.

b) Where Supplier Advocates are physically present to engage Children and Young People at each session (individually or in a group).

c) The session must include:

- An explanation that every Child and Young Person continues to have rights, under the UNCRC or Human Rights Act 1998.
- An summary of those rights that are particularly relevant to Children and Young People in custody and that align with Advocacy – such as UNCRC Articles 2, 3, 8, and 12 (UNCRC) and Human Rights Act Articles 8, 9, 10, 14 and Protocol 1, Articles 1 and 2.
- An explanation that every staff member working in youth custody also has rights under the Human Rights Act.
- The champion and promotion of opportunities for Children and Young People to constructively participate in promoting their own rights and protecting those of others.

1.4.3 The sessions should be of sufficient time to achieve the above and to ensure that all Children and Young People who wish to voice a view to the Supplier's Staff are able to do so. These will need to be planned and agreed with each Secure Establishment as a part of the Induction Programme for Children and Young People.

1.4.4 The Supplier must make any materials developed for Children and Young Peoples' Rights awareness sessions available to all Children and Young People at the Secure Establishments – this should be co-created with Children and Young People so that the information is accessible and in a range of formats, including digital.

1.5 Unit Visits

1.5.1 As part of Advocacy Services being visible and accessible to all Children and Young People, the Supplier's Staff are required to undertake at least the minimum agreed number of Unit Visits to each residential unit and wing in use for Children and Young People within each Secure Establishment in scope of these Services, including healthcare units, enhanced support units, and care and separation units – see Schedule 7 (Secure Establishments).

1.5.2 A Unit Visit is defined as:

a) Advocates are physically present and visible to Children and Young People living and staff working on the Unit.

b) Advocates speaking individually to any Children and Young People whom Secure Establishment staff on the Unit raise specific concerns about.

c) Advocates shall specifically visit any Child or Young Person separated and remaining in their bedroom, whether through a sanction or by choice, when it is appropriate to do so.

d) Advocates spend sufficient time on each Unit Visit to achieve the above and ensure that all Children and Young People who wish to see the Supplier's Staff are able to do so.

1.5.3 Unit Visits should be:

a) Planned – so that these consider and target times when Children and Young People will be available.

b) Regular – so that accessibility and availability of Advocates is demonstrated, and to reduce the time required to achieve necessary activity on each Unit Visit.

c) Publicised – so that Children and Young People and staff know when to expect Advocates.

1.5.4 The Supplier must consider the different regimes within each Secure Establishment, including but not limited to:

a) The times when Children and Young People will be locked in their bedrooms.

b) Times when rooms / space for privacy and / or sensitive discussion can be had.

c) When Children and Young People prefer to see the Supplier's Staff, including during their evening association time and/ or at weekends.

1.5.5 Where the planned schedule of Unit Visits has to change – either in exception, or to move to a different scheduled day/ time – the Supplier is responsible for ensuring Children and Young People and staff know of this.

1.5.6 So that Children and Young People become accustomed to and can more easily recognise Advocates, Advocates should regularly visit the same units or wings of Secure Establishments.

1.6 Referrals to Advocacy Services

1.6.1 The Service is to be delivered, and the Supplier will manage referrals for Children and Young People, via "Cases". For each Child or Young Person referral to the Service (for every Case) the Supplier will explain to the Child or Young Person:

a) The Service's confidentiality statement.

b) What information the Supplier holds about the Child or Young Person and who can access it, as well as the Child or Young Person's rights to access their own personal information.

c) How the Child or Young Person can make a complaint about the Services.

1.6.2 Children and Young People should be able to access the service 24 hours a day whilst in the Secure Establishment and the Supplier shall respond to all referrals, and provide advice and assistance without delay when contacted, within a maximum of 72 hours from the point of notification.

1.6.3 The Supplier shall provide regular and frequent feedback to Children and Young People on any issues which they are being supported on and they will ensure Children and Young People are made aware of the timescales in which they can expect feedback and are provided with further information or updates as soon as is practicable.

1.6.4 The Supplier shall establish on commencement of engagement with a Child or Young Person their preferred outcome/s and their preferred level and methods of engagement required by the Supplier's Staff – including physical and digital methods. For all Cases that will take Advocates longer than 30 minutes to resolve, an Advocacy Plan should be agreed with the Child or Young Person so that they understand and have a documented record of the support and help they have agreed that the Services will provide and should be reviewed at each stage of the Case in partnership with the Child or Young Person.

1.6.5 The Supplier shall provide constructive support that is focused on strengths-based development and that is customised to the individual identity of the Child or Young Person. Services shall recognise the importance of diversity in helping to equip each Child and Young Person with the skills and confidence to advocate for themselves.

1.6.6 The Supplier will make appropriate arrangements to ensure that any Child or Young Person who requires interpretation services to fully access and understand Advocacy Services has this in place. In most cases, the Child or Young Person will be able to access the Secure Establishment facilities for interpretation services – though the Supplier will have to agree and arrange its use with the Secure Establishment (See Schedule 12 (Local Protocols). For the avoidance of doubt:

a) Any separate interpretation services the Supplier provides in delivering the Services to Children and Young People will be the responsibility of and at the cost of the Supplier.

b) Where the interaction with the Child or Young Person is organised or led by the Secure Establishment but at which the Child or Young Person has asked an Advocate to be present (e.g. casework or safeguarding meetings, searches or restraint debriefs, etc) then the associated responsibility and cost for interpretation services will sit with the Secure Establishment.

1.6.7 The Supplier will offer a broad range of support to Children and Young People to achieve the outcomes for this Section 1, which will include coordinating access and supporting referrals to other services and agencies who have responsibilities to assist Children and Young People in resolving their issues.

1.6.8 The Supplier shall manage Children and Young People's expectations realistically and shall advocate for/ assist the Child or Young Person to advocate for themselves on any issue they request. This will include but will not be limited to assisting Children and Young People to make informal and formal requests, representations, and complaints in their dealings with Secure Establishment staff and external agencies.

1.6.9 Where a Child or Young Person requests it (and it is appropriate to the role of an Advocate), the Supplier will accompany the Child or Young Person to meetings at the Secure Establishment to support them to represent their views and wishes. Advocates should not attend meetings on a Child or Young Person's behalf where that Child or Young Person is not invited and able to be present. The Supplier is required to work with the Secure Establishment to ensure that such meetings are held when Advocates can be available to attend. In these instances, the Supplier's Staff shall inform the Child or Young Person that such requests will require 3 Calendar Days' notice (non-urgent referral), with the exception of where a request has clear safeguarding implications, where a request may be received with one calendar days' notice.

1.6.10 Advocacy support for Children and Young people in custody can include helping them through Secure Establishment procedures and processes – such as those areas highlighted in Section 4 of this Schedule.

1.7 Children and Young People's Councils / Forums and Consultations

1.7.1 Secure Establishments may have established Children and Young People's forums and council style groups to listen to the views of Children and Young People. These provide Children and Young People with an opportunity whilst in custody to drive change and/or improvements in the day-to-day care and support they receive in the Secure Establishment. Secure Establishments may also hold specific or regular consultations to understand Children and Young Peoples' views.

1.7.2 The Supplier shall, where appropriate to their role, offer to support Children and Young People at these councils and forums in and consultations with the Secure Establishment: to assist them in being able to express their wishes and feelings; and to pursue through a collaborative and coordinated approach, with the Secure Establishment, appropriate courses of action to enable attendance of Advocates.

1.8 Children and Young People Leaving the Secure Establishment – release, move/ transfer or transition

1.8.1 All Children and Young People who engage with the Suppler Services will at some point leave the Secure Establishment: being released (usually on licence) into their community; in moving to another Secure Establishment; or in transitioning to adult custody. For Children and Young People who are engaged with the Supplier as Live Cases at these times, support should be offered and any concerns the Child or Young Person has listened to.

1.8.2 Youth Offending Team (YOT) case managers have responsibility for overall case management of Children on community and custodial orders, and joint accountability with the Secure Establishment for sentence planning and delivery. Probation Services similarly have overall case management responsibility for adults in communities (including 18 year olds, where the YOT has transferred the case).[3] The Supplier shall establish, as part of Local Protocols (See Section 4 of this Specification) effective working arrangements with the Secure Establishment Resettlement Practitioner / case work team, to support those Children and Young People whom the Supplier is working with (advocacy cases) to actively engage with their sentence / remand plan, and support them to contribute their views and wishes.

1.8.3 The Supplier should also be prepared for the handover of Children and Young People's (Live) cases to YOTs or community-based advocacy providers, for those who are due to be released into communities and where this aligns with their wishes and views. The Supplier should provide each Child and Young Person accessing the Services with information about who they can contact on release. The Child or Young Person must be consulted with before any action is taken for the handover of their case and permission must be granted for any transfer of their information.

1.8.4 If a Child or Young Person working with the Supplier (a Live Case) is due to be moved to another Secure Establishment,[4] the Supplier must ensure that the individual's case note file/ Advocacy Plan is updated and made ready for transfer. Any outstanding actions that need to be continued must be highlighted along with timeframes for completion. The Supplier must communicate with the Child and Young Person any outstanding actions and agree with them how these will be taken forward at their new Secure Establishment – including transferring the case to Supplier or other advocates working at the receiving Secure Establishment. The Supplier's Staff must seek consent from the Child or Young Person before engagement with other agencies can begin (on the Child or Young Person's behalf).

[3] Custody and resettlement: section 7 case management guidance - GOV.UK (www.gov.uk)
Case management guidance - Custody and resettlement - Guidance - GOV.UK (www.gov.uk)

[4] Placing young people in custody: guide for youth justice practitioners - GOV.UK (www.gov.uk)

1.8.5 This includes the Supplier liaising with local authority commissioned advocacy services to arrange for the transfer of open cases if a Child or Young Person is to transfer to a Secure Children's Home (SCH).

1.8.6 If a Young Person working with the Supplier (Live Case) is due to transition to adult custody,[5] the above process for a Child or Young Person moving to another Secure Establishment remains relevant – though it is unlikely that advocacy services will be directly provided in adult custody, existing means of statutory and custody support will be available, as will access to Samaritans, national helplines and other health and wellbeing support.

1.8.7 The Supplier shall inform the Child or Young Person of the processes outlined above (as applicable to their Case) in paragraphs 1.8.4 to 1.8.6 and seek their permission to transfer their personal information, in accordance with the Supplier's confidentiality processes and in compliance with Data Protection Law.

1.8.8 The Supplier must inform the Child or Young Person of who their new Advocate will be and how to contact them.

1.9 Non-Instructed advocacy

1.9.1 The Supplier should always engage Children and Young People presuming that they are able to communicate their views and wishes directly. Where there is evidence that a Child or Young Person lacks capacity to instruct a Supplier Advocate on a specific issue, non-instructed advocacy can act as a safeguard against not knowing or understanding their rights. The Supplier's Staff shall coordinate any such work with the Child or Young Person, through effective casework and communication, and look to develop with them the skills to advocate for themselves in future.

1.9.2 The Supplier will also work with the Child or Young person to ensure that other professionals at each Secure Establishments who have a responsibility and remit to support them are included – such as the Special Education Needs Coordinator and health-care professionals.

1.10 Ad hoc Services

1.10.1 The Authority shall seek the Supplier's assistance in ad hoc Service provisions that represent the voice and/ or views of Children and Young People in custody – this may include Children and Young People who are not (at these times) using the Services – such as carrying out specific consultations or providing specific information and support (See also Section 2 of this Specification). The Authority will negotiate such ad hoc Services with the Supplier when required.

1.11 The provision of Services will be aided by the use of an electronic case management system.

1.11.1 The Supplier shall carry out the terms of the Contract and facilitate the Service through use of their electronic case management system suitable for the needs of this specification.

1.11.2 The Supplier will record and store case management data electronically. The system will only be accessible by the Supplier. All data will be stored in physically secure locations in Secure Establishments or named places of business.

[5] Transition of Young People from the Children and Young People Secure Estate to Adult Custody Policy Framework - GOV.UK (www.gov.uk)

1.11.3 The Supplier is required to record information about the Child and Young Person cases they are working on. This will include, where necessary, cases with references to Secure Establishment staff and staff working for other organisations at the Secure Establishment – for instance, to detail Supplier conversations with staff about a Child or Young Person, or to detail any allegations made by a Child or Young Person against a staff member.
1.11.4 At all times the electronic case management system and case recording procedures used by the Supplier will comply with all information assurance and security requirements as at Schedule 6 (Information Security & Assurance) and Data Protection Law.

1.11.5 The electronic case management system will have such functionality so as to comply with the requirements of clause H8 (Retendering and Handover) and H9 (Exit Management) at the point of retendering and handover or exit. In compliance with clause H8.8, should handover be required, the Supplier shall ensure that all data and information held on Live Cases is transferred to any person designated by the Authority.

1.11.6 At the point of exit, any cases which are not considered Live Cases will be archived and transferred back to the Authority in accordance with clause H8 (Retendering and Handover) and H9 (Exit Management).

Section 2 : Safeguarding and Protecting Children and Young People

Outcomes
• Children and Young People are safeguarded. • Children and Young People in Wales are safeguarded in line with Wales Safeguarding Procedures. • Children and Young People are informed if an advocate deems a safeguarding or child protection referral necessary, their consent sought, and advocacy support maintained where the Child or Young Persons requires this. • Children and Young People are aware that – alongside the outcomes above – there are conditions under which the Supplier must make a disclosure.
Service Requirements
2.1 The Supplier shall provide a Service that is confidential and will comply with relevant statutory guidance in relation to safeguarding and child protection. The Supplier's Staff shall ensure through each Child and Young Person's introduction to, and in information provided to them about, the Services (see Section 1 of this Specification) that Children and Young People are clear of the confidentiality statement and the limits to this. 2.2 Under statutory guidance, there are certain and necessary limits to the Supplier's confidentiality, which will be exercised when the Supplier's Staff is made aware of any:

a) Risk of harm to the Child or Young Person – from themselves, or from any other Child or Young Person, or from any staff member or other person within or outside of the Secure Establishment;
b) Risk of harm to any other person from the Child or Young Person the Advocate is working with; and/or
c) Risk to security of the Secure Establishment.

In the instances outlined above, the Supplier will follow the Local Protocols applicable to the Secure Establishment in which the Child or Young Person is accommodated, to refer any safeguarding or security concerns as soon as is reasonably practicable to ensure appropriate safeguarding action is taken and before the Supplier leaving the Secure Establishment.

This includes concern that would come under the National Referral Mechanism (NRM) framework[6] for identifying and referring potential victims of modern slavery and ensuring they receive the appropriate support. Advocates are not required or expected to make NRM referrals themselves for Children or Young People, but may be asked to support a Child or Young Person for whom NRM is a concern/ issue, including with a referral.

2.3 The Supplier shall develop relationships with and have in place a clear process for the reporting, under statute and if required by circumstances, of safeguarding incidents and child protection referrals direct to the Local Authority Designated Officer (LADO) or Designated Safeguarding Person for each Secure Establishment. These referrals will always be authorised by the Supplier's Senior Management Team and the Secure Establishment must be informed when such a referral has taken place. Where allegations are made against Secure Establishment staff members, these will be passed on to the Secure Establishment as a safeguarding referral, in line with the Local Protocols.

2.4 The Supplier shall remind Children and Young People of confidentiality and seek their consent to share any personal information given by the Child or Young Person that is needed to assist them. A record of the Child or Young Person's consent must be maintained securely on the Supplier's information system. Where a Child or Young Person does not give their consent, Advocates will not share any information except where there is a risk of harm as described in paragraph 2.2.

2.5 The Supplier must comply with relevant Data Protection Law, including in instances where a Child or Young Person declines consent for their information to be stored or shared.

2.6 The Supplier shall implement a clear process that enables the Supplier's Staff to raise concerns immediately about a Child or Young Person's safety and wellbeing, and to follow this up with a referral if necessary.

2.7 The Supplier shall provide the Authority with assurance that safeguarding, and child protection incidents have been reported and that any learning from incidents is considered and acted upon.

2.8 The Supplier shall have in place and shall review at least annually safeguarding and child protection policies and processes. These must be subject to scrutiny independent of the Supplier.

2.9 The Supplier shall develop relationships with the Local Safeguarding Children's Partnerships (LSCPs) for England and the Regional Safeguarding Boards (RSB) for Wales that cover each Secure Establishment for advice and guidance on their policies and processes (this shall be agreed with LSCPs / RSBs).

[6] National referral mechanism guidance: adult (England and Wales) - GOV.UK (www.gov.uk)

2.10 The Supplier shall ensure its approach to safeguarding and child protection includes a clear process for learning lessons which shall feed into any reviews and updates of safeguarding and child protection policy and practice. This includes a requirement to share learning with partners, including the LSCPs or RSBs and the Authority.

2.11 The Supplier shall develop sufficient plans to be able to reasonably respond to an Authority request to (re)allocate/ provide additional resources to support Children and Young People in the event of a serious incident at a Secure Establishment. The Supplier will agree with Secure Establishments as part of Local Protocols any notification process for alerting onsite Advocates of incidents that risk the safety or security of staff or the Services.

Section 3 : Staffing, Leadership and Management

Outcomes
Advocates and managers understand the purpose of the Service, their boundaries and lines of accountability and are trained to a high standard to undertake their roles effectively.
Service Requirements
3.1 Staff Solution 3.1.1 The Supplier's Staff have the appropriate experience, skills and qualifications to work with Children and Young People. All of the Supplier's Staff have a desire to work with Children and Young People and shall behave as positive role models. 3.1.2 The Supplier shall provide a sufficient staffing solution at each Secure Establishment that has the ability to meet the Authority's requirements of the Service, including fluctuations in demand and to provide cover as required to enable continued service delivery for periods of leave, long-term sickness, maternity leave, and departure/ recruitment. The Supplier will ensure an effective Business Continuity Plan (in accordance with Schedule 11 (Business Continuity Plan)) is in place to maintain delivery of service to Children and Young People that considers, but is not limited to, restricted physical access to Children and Young People in the Secure Establishment. 3.1.3 The Supplier shall provide its Staff with easily accessible information that sets out the Supplier's expectations of their Staff whilst conducting their roles in the delivery of Services under this Contract. This information will include, but may not be limited to: a) Code of conduct and behaviour; b) Supervision and Support; c) Lone working; d) The use of social media including, but not limited to: internet sites, mobile telephones and email; and e) Guidelines for Staff and the Service to remain fully independent (of Secure Establishment operators). 3.1.4 All Supplier's Staff working with Children and Young People must be appropriately vetted for their role, including security clearances required in accordance with clause B5.5 of this Contract, and by Safer recruitment practices (see paragraph 3.2 below). This will include (but may not be limited to): a) Baseline Personnel Security Standard (BPSS); and b) Enhanced Disclosure and Barring Service (DBS) 3.1.5 All Supplier's Staff working in STCs shall be subject to appointment by the Authority as an Independent Person under STC Rules. [7]

[7] Rule 44 of the Secure Training Centre Rules 1998

3.1.6 The Supplier shall comply with the security clearance requirements of each Secure Establishment where its staff will be located and will ensure that it considers the time required for these requirements when recruiting or renewing security clearances for Staff.

3.2 Recruitment

3.2.1 The Supplier shall have in place policies and structures that deliver and promote Safer recruitment practices for Staff/ roles working directly with Children and Young People.

3.2.2 The Supplier shall have a recruitment and selection policy to attract a diverse and skilled workforce committed to working with Children and Young People. The Supplier must consider the ethnic, gender, cultural and language identities of Children and Young People at Secure Establishments and aim to provide Staff who reflect these.

3.2.3 When recruiting Staff, the Supplier shall comply in all respects with the 1992 Warner Report "Choosing with Care" and any subsequent relevant recommendations for recruitment, selection and training of staff dealing with Children and Young People in custody.

3.3 Staff Training

3.3.1 The Supplier shall provide all Staff with an induction and training programme to ensure that they are equipped with the necessary skills to deliver the Service.

3.3.1A The Supplier shall ensure that an effective supervision system is in place to support the Staff to maintain their wellbeing throughout both the routine operation of their duties and as a result of any occurrence of events or incidents within the Secure establishments, including supervision and peer support.

3.3.2 The Supplier shall develop and implement a learning and development plan which enables the development needs of each individual Staff member to be met through structured and informal training and supervision to ensure the skills and competence of Staff are being developed and maintained.

3.3.3 The Supplier will ensure that all Advocates are trained as minimum in the following areas:

a) Advocacy skills
b) Children's and Human Rights
c) Safeguarding and child protection
d) Adverse Childhood Experiences (ACEs) / Trauma Informed Practices (TiP)
e) Looked after children
f) Mental health awareness
g) Speech, language, and communication needs of Young People
h) Familiarisation with the youth justice system, the agencies involved internally and externally to youth custody
i) The Service should also have at least one Advocate available to Children and Young People at each Secure Establishment who has been trained on non-instructed advocacy.

3.3.4 The Secure Establishments may require the Supplier's Staff to attend specific training programmes directly linked to Secure Establishment practices and procedures. Whilst the costs of delivering this training will be covered by the Secure Establishment, the Supplier shall be required to bear the costs of providing its Staff. Training may cover the following areas:

a) Security and key handling

b) Personal protection

c) On site health & safety awareness.

d) Building Bridges

e) SECURE STAIRS (England) NHS commissioning » Children and young people (england.nhs.uk)

f) TRACE (Wales) TrACE Organisation Self-Assessment Tool 1a (002).pdf (gov.wales)

g) Assessment Care in Custody and Teamwork (ACCT) for YOIs

h) Suicide and Self-Harm (SASH) for STCs

i) Minimising and Managing Physical Restraint (MMPR)

j) Custody Support Plan (CuSP)

3.3.5 The Supplier shall ensure that their Staff are provided with ongoing continuing professional development and refreshed training throughout the duration of the Contract.

3.4 Management Structure

3.4.1 The Supplier shall ensure that all of its Staff are supported by management structures that offer clear lines of accountability and escalation.

3.4.2 The Supplier shall ensure that Children and Young People are recipients of an Advocacy Service that is led by a motivated and focussed leadership, who champion the rights of the Children and Young People in youth custody, lead by example and have the experience, understanding an ability to effectively and efficiently deliver the Services in accordance with the Authority's requirements set out in the Specification and the Contract.

3.4.3 The Supplier shall provide sufficient management resource to manage and support the Service providing a single point of contact for the Authority.

3.5 Staffing Processes

3.5.1 The Supplier shall ensure it has effective procedures in place to manage Staff performance, attendance, and conduct. The Supplier shall ensure that it has conduct procedures that have due regard to the safety and protection of Children and Young People. Where the Supplier is investigating Staff for any poor conduct that calls into question their suitability to work on the Service the Supplier will inform the Authority of the investigation and the outcome.

3.5.2 The Supplier shall have fair and effective whistle-blowing procedures in place, to support its Staff who wish to make any allegation or raise any legitimate concerns they may have about the conduct of their colleagues or organisation's management without fear of jeopardising their own prospects and position.

Section 4 : Working with Secure Establishments and Other Services for Children and Young People

Outcomes
Children and Young People accessing Advocacy Services are aware their rights are championed with other professionals and adults working with Children and Young People.
Service Requirements
4.1 Working in Secure Establishments 4.1.1 The Supplier will be provided free of charge in each of the Secure Establishments with office space suitably furnished for the Supplier's Staff use. The size and location of such space is at the discretion of each Secure Establishment and may be moved as part of usual reconfiguration of office/ Staff spaces. 4.1.2 The provision of internet and/ or telephone connection in the (Supplier's) office at each Secure Establishment will be the responsibility of the Supplier to both install and pay for, if/ as required. 4.1.3 Where the Supplier office location is required by the Secure Establishment to be moved, as part of usual reconfiguration of office / Staff spaces, the Secure Establishment will be responsible for any reconnection costs for internet and telephone. 4.1.4 The scope and provision of such ICT connections will be subject to approval by the Authority before installation – specifically with HMPPS Information Assurance Team. 4.2 Working with Secure Establishments 4.2.1 The Supplier shall ensure that it develops an understanding of the secure environment and builds constructive working relationships on a day-to-day basis with Secure Establishment staff, across the full range of Services operating within the STC or YOI, to empower Children and Young People to get the earliest and best possible resolution to the issues that have been raised whilst maintaining their independence from the Authority and the secure estate provider at all times. 4.2.2 The Supplier will comply with all relevant Secure Establishment procedures, particularly those related to security, Safeguarding and health and safety. 4.2.3 The Supplier shall ensure that they follow the policies and processes in place to avoid duplication of the roles and responsibilities of other professionals within the Secure Establishment such as social care services, safeguarding teams or case managers where these are in place and flag concerns to the Authority. 4.2.4 The Supplier shall assist Children and Young People with understanding, accessing, and using Secure Establishment processes where requested by the Child or Young Person. The Supplier shall work effectively and constructively with individual Secure Establishments to establish effective communication methods that support timely and responsive Advocacy Services, including, but is not limited to: a) Notification of Children and Young People who are new arrivals to the Secure Establishment, and the Child or Young Person's location within the Secure Establishment; b) Referral of any Child or Young Person where Secure Establishment staff identify that the Child or Young Person should be visited by the Supplier's Staff and their location; and

c) Referral of any Child or Young Person following a full search or where a Serious Injury and Warning Sign (SIWS) is activated post restraint.

4.2.5 The Supplier shall work with each Secure Establishment to ensure that members of Staff and other Secure Establishment service providers understand the role of the Advocacy Services and the referral pathways available. This may include, but is not limited to:

a) Meeting new staff within the Secure Establishment during their induction course and providing briefings as required;

b) Providing information to new Secure Establishment staff outlining both the service and how to make referrals, and

c) Offer training / briefing sessions related to the Service (e.g. principles of advocacy, or Children & Human Rights) to existing Secure Establishment staff.

4.2.6 Where required, the Supplier shall work collaboratively with Secure Establishments at each site to ensure the smooth provision of Services.

4.3 Contacting the Service

4.3.1 While the Service is predominantly Child and Young Person led, anyone can make a referral to the Advocacy Service on behalf of a Child or Young Person. The Supplier's Staff will actively encourage and enable all relevant agencies and adults who are in a position to advise Children and Young People to:

a) Inform Children and Young People about the Service;

b) Encourage them to use it;

c) Help them to contact it.

4.3.2 Routes of contacting the Service will be facilitated by the Supplier that will include but should not be limited to:

a) Self-referral – the Authority expects the majority of referrals to be from Children and Young People, as a Child and Young Person led service;

b) Secure Establishment (Custody Operator) staff – including Safeguarding, Resettlement Practitioner/ Casework and MMPR teams;

c) Health professionals, Education provider, Religious Leaders;

d) Social workers, Youth Offending Teams (YOTs – or Probation Workers as relevant), youth workers and Police Officers.

e) Children and Young Peoples' families, carers, and friends. Other professionals and people involved in the support and care of the Child or Young Person – either internal or external to the Secure Establishment.

4.3.3 The Supplier shall provide methods of contact in order that referrals can be received from the above and it will publicise these methods appropriately across, and in partnership with, the Secure Establishment so that these are accessible to relevant agencies and adults as well as all Children and Young People.

4.3.4 The Suppliers' Staff shall check with establishment/ residential staff whether they have any specific concerns with regards to a Child or Young Person who might benefit from the Service. The Supplier's Staff shall speak to that Child or Young Person individually and, if necessary, remind them of how the Service works, what support it can offer and how to make contact.

4.3.5 The Supplier should minimise any impact on Children and Young Peoples' education by trying, where possible and where the matter is non-urgent, to contact Children and Young People outside of planned education hours, i.e. before education, during lunch breaks or in the evenings or at weekends.

4.4 Local Protocols:

4.4.1 The Supplier shall agree a local Protocol agreement with each Secure Establishment to help facilitate provision of the Services, in line with Schedule 12(Local Protocols) during the mobilisation phase of the Services, which shall be set out in the Detailed Mobilisation Plan.

4.4.2 The content of each Local Protocol shall include, but is not limited to:

a) Outlining expectations and requirements of Supplier's Staff when working in a secure environment and any local arrangements needed regarding key/ radio training etc;
b) Advertising the Services across the Secure Establishment;
c) Receiving timely notifications of a Child or Young Person newly arrived at a Secure Establishment, including details of acute needs or risk assessment;
d) Receiving timely notifications of a Child or Young Person for whom an urgent request is made, including: Following any full search at a Secure Establishment, or where the Serious Injury and Warning Sign (SIWS) procedure is activated, following restraint;
e) For whom any referral is made by Secure Establishment or other staff to the Supplier requesting Advocacy Workers visit the Child and Young Person;
f) Delivery of Children and Human Rights Sessions and the minimum Unit Visits.

4.4.3 Such protocols shall be reviewed annually, co-created with partners and Children and Young People, and made available to the Authority upon request.

4.4.4 The Supplier shall work with the Authority to review, refresh and agree the Local Protocols in accordance with Schedule 12 (Local Protocols) so these reflect working in partnership and business practices, as part of annual business planning.

4.4.5 Should there be a change in the custodial operator at any Secure Establishment where the Supplier is delivering an Advocacy Service, then the Supplier will work the outgoing operator and the incoming operator to ensure the Advocacy Service continues to deliver effectively and that Local Protocols transition as appropriate.

4.5 Support during Secure Establishment Procedures (Adjudications - YOIs only)

4.5.1 As per Section 1 of this Specification, Advocacy Services may as part of the support provided to Children and Young People be required to help them navigate through Secure Establishment procedures. For example, in YOIs this could involve the adjudications process[8].

8 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1154896/psi-05-2018-prison-adjudications-may-2023.pdf

4.5.2 Secure Establishments are required to provide Children and Young People subject to restraint with an opportunity to debrief and discuss the behaviour that led up to the restraint. The procedure for debriefs includes that Secure Establishment staff ask the Child or Young Person whether they would like the support of an Advocate, including at any debrief. Similarly, in YOIs, a Child or Young Person subject to the adjudication procedure should be asked by Secure Establishment staff if they would like advocacy support and an Advocate present at their adjudication. In such cases, the Supplier shall work collaboratively with the Secure Establishment to avoid undue delays to these procedures.

4.5.3 Where a request for advocacy support is made relating to attending a specific meeting or forum, the Child or Young Person and/or Secure Establishment should ideally provide the Supplier with at least 72 hours' notice (the contractual timeframe for responding to referrals), except where this relates to an urgent request – in which cases, the Supplier has 24 hours to respond. The notice period for referrals provides Advocates with a window of opportunity to contact the Child or Young Person ahead of any procedural meeting/ forum, in order that the support can be informed and tailored to the individual.

4.6 Serious Injury Warning Signs and Full Searches

4.6.1 Where the Advocacy Service is notified that a Child or Young Person has either:

a) been subject to a full search; or,

b) been involved in a restraint which resulted in a Serious Injury Warning Sign report being generated

Then the notification will be treated as an Urgent Referral and the Supplier shall ensure that an Advocate will make contact with the Child or Young Person within 24 hours of receiving the notification.

4.7 Raising awareness of the issues facing Children and Young People in custody

4.7.1 The Supplier will have a system for raising awareness of the issues facing Children and Young People in custody in order to promote resolution and prevention at local and systemic levels.

4.7.2 The Supplier shall arrange with each Secure Establishment's nominated senior management team lead/ link at site for Advocacy Services (known in YOIs as the Service Liaison Governor) to hold Advocacy Review Meetings (ARMs) at least monthly. These meetings will be used to highlight thematic issues that Children and Young People have identified to the Supplier over the preceding period and to work collaboratively with the Secure Establishment to find solutions.

4.7.3 The Supplier shall also submit Monthly Data Returns, Quarterly Contract Management Reports and an Annual Report highlighting the number and type of issues being raised by Children and Young People at each Secure Establishment and across the Service (see Section 5 of this Specification and paragraph 3 of Schedule 10 (Performance Mechanism).

4.8 Working with Children and Young People's families / carers and significant others

4.8.1 The Supplier shall work with the Secure Establishment to publicise the Service to the families / carers and significant others of Children and Young People such that they are aware of the support the Service can provide and how they can contact the Service if they feel the need to make a referral for a Child or Young Person in custody.

4.9 Working with stakeholders external to the Secure Establishment.

4.9.1 The Supplier shall develop constructive working relationships with a wide range of relevant external organisations so that they can also support Children and Young People to find the earliest

possible positive resolution of their issues and concerns – being mindful of the Service Requirement at paragraph 4.2 of this Section 4 and working with Secure Establishment staff/ functions.

Section 5 : Performance Management, Service Assurance and Improvement

Outcomes
• Children and Young People receive a service which: – is monitored for quality; – enables and encourages them to give feedback; – generates information which can be used for service improvements. • Children and Young People can express their views about the Advocacy Service they receive and can affect the way the Services they receive are delivered. • Children and Young People who are appropriate to representing themselves and their peers are involved in Service evaluation, development and improvement and are supported in their choice of how to contribute.
Service Requirements
<u>5.1 Performance reviews</u> 5.1.1 The Authority will seek assurance that the Service is being delivered in accordance with the Authority's requirements. Performance reviews shall form part of the Authority's regular contractual management and monitoring function. 5.1.2 The Supplier shall facilitate and engage with such performance reviews as stipulated in paragraph 3 of Schedule 10 (Performance Mechanism), by: a) Providing the management information; b) Participating in the Contract Review Meetings with the Authority – used primarily to assess the Supplier's performance over the Performance Quarter but also to highlight thematic issues that the Supplier has identified from supporting Children and Young People; and c) Provision of Quarterly Contract Management Reports. <u>5.2 Complaints in relation to the Advocacy Service</u> 5.2.1 The Supplier shall ensure it has a confidential complaints process in place detailing how the procedure can be accessed and the expected timescales in line with Supplier policy for responses. 5.2.2 The complaints process shall: a) Be publicised to Children and Young People and staff in each Secure Establishment to allow these and external agencies to make complaints about the Advocacy Service or Staff;

b) Be accessible through a variety of ways and the information provided should be available in formats and languages as well as consider any additional needs that Children and Young People, or others, may have in accessing and understanding the complaints process;

c) Allow for timely and appropriate replies to be made to the complainant and for any lessons learned to be assessed and implemented and shared with the Authority.

5.2.3 The Supplier shall support and empower Children and Young People who wish to, to use the complaints procedure and shall respect their rights to do so.

5.2.4 The Supplier should also provide Children and Young People with details about other opportunities for information, advice, and assistance and/or support about how to complain about the Advocacy Services, including the local authority (for the Secure Establishment) and, in Wales, the Children's Commissioner for Wales. [9]

5.2.5 The Supplier shall regularly review complaints received to identify any emerging key themes and issues and develop plans to improve the Service.

5.3 Reports and delivery plans.

5.3.1 The Supplier shall provide Monthly data on the Service provided at each Secure Establishment, to be submitted to the Authority by the seventh (7th) calendar day after the end of the Month.

5.3.2 The Supplier shall provide Quarterly Contract Management Reports on the delivery of the Service, which will include a Monthly Data Report on each Secure Establishment, in accordance with Schedule 7 (Secure Establishments). The reports should highlight contractual performance, thematic issues, trends, and feedback from Children and Young People. These reports will be submitted to the Authority by the seventh (7th) calendar day after the end of each Performance Quarter. Where appropriate, the Supplier will work with the Authority and the Secure Establishment and other stakeholders to explore and promote solutions to any thematic or systemic issues.

The Supplier's report templates – provided to and approved by the Authority during mobilisation –must be used as the basis of the reports .

5.3.3 The Supplier shall be required to provide an Annual Report detailing an overview of the Service it provides both nationally and at establishment level, highlighting any key thematic issues or trends – including for Children and Young People in Wales and in England. Data about the views of Children and Young People and any complaints made by them will be included in this analysis. In addition, the Annual Report will detail the annual service delivery plan for the coming year, showing how lessons learned are being employed to improve the Service and develop advocacy practices.

5.3.4 A draft Annual report will be submitted to the Authority within 6 weeks after the end of the Contract Year, and a final report, based on feedback from the Authority, will be submitted within 10 weeks after the end of the Contract Year.

[9] Independent Professional Advocacy cover English (gov.wales).

The Children's Commissioner for England defers complaints to be made through the Local Authority – Contact us | Children's Commissioner for England (childrenscommissioner.gov.uk)).

5.3.5 The Authority will work with the Supplier to agree a version of the Annual Report suitable for sharing with key external partners – such as local authorities hosting Secure Establishments – and publication.

5.3.6 The Supplier shall be required to provide the Authority 4 weeks prior to end of the Contract Year with a service delivery plan for the following Contract Year.

5.4 Information Management

5.4.1 The Supplier shall share information with the Authority in a timely manner regarding press releases, official communications, and other media activities regarding the Service.

5.5 Quality Assurance

5.5.1 The Supplier will have effective quality assurance processes in place to ensure that all requirements are met and to strive for continuous service improvement. The quality processes will include seeking feedback from Children and Young People who have used the service at the Secure Establishment.

5.5.2 The Supplier shall have a quality assurance (QA) system in place for the Service and processes shall be in place which engage and support all Supplier's Staff in improving practices. The Supplier shall ensure its quality assurance system includes self-monitoring and internal reporting of the quality of services delivered including performance checks, frequency, and scope. It shall as a minimum demonstrate:

a) The requirements of this Schedule;

b) How Children and Young People participate in the design, planning, delivery monitoring and evaluation of Advocacy Services, including those steps taken by the Supplier to reach out to promote access to underrepresented groups;

c) Produce an annual plan detailing how and when QA reviews/audits will be conducted; and

d) Demonstrate the frequency in which the QA system will be reviewed.

5.5.3 The Supplier shall provide detailed information to the Authority about the annual plan, any issues identified by the QA system, its associated audit processes, and response plans.

5.5.4 The Supplier shall develop a framework for the quality management of the Service including:

a) Data collection and analysis that aligns with Authority requirements;

b) Monitoring and evaluation which is both practical and informative.

5.5.5 The Supplier shall take reasonable endeavours to continuously improve service delivery, including the identification of key themes and issues raised by Children and Young People to support Service change.

OPTIONAL SERVICES

These Optional Services are only required where the Authority activates such, using such Change control mechanisms as there are agreed in this Contract (clause F4 (Change)).

Section 6 : Support for Children and Young People following Youth Custody

Outcomes
Release Support • Children and Young People understand how Release Support provided by the independent advocacy service works exclusively for them and can help them. • Children and Young People accessing Release Support are empowered to have their views and wishes heard and their rights respected. • Children and Young People are supported, prepared and are more confident when presenting their views directly to decision makers. • Children and Young People accessing Release Support are aware their rights are championed with other professionals and adults working with Children and Young People in their communities. • Children and Young People can express their views about the Release Support they receive and can affect the way the Services they receive are delivered. *Follow-on Interviews* • Children and Young People understand and are confident that their privacy and confidentiality will be respected throughout the Follow-on Interview process. • Children and Young People are informed if a safeguarding or child protection referral is deemed necessary and their consent sought. • Children and Young People are aware that there are conditions under which Advocacy Services must make a disclosure. • Children and Young People able to represent themselves and their peers are involved in Follow-on Interview service evaluation, development and improvement and are supported in their choice of how to contribute.
Service Requirements

6.1 Release Support

6.1.1 The Supplier is required, as stipulated in paragraph 1.8 of Section 1 of this Specification (Children and Young People Leaving the Secure Establishment) to support all Children and Young People whom the Supplier is working with (advocacy cases) whilst they remain in youth custody, whether to resettle back into their communities, or if transitioning to adult custody or moving to another Secure Establishment.

6.1.2 This Release Support service is to continue to provide advocacy support directly to the Child or Young Person in their community, following their release from the Secure Establishment. The principles and standards governing advocacy – providing confidential, independent support – therefore continue to apply to this Optional Service.

6.1.3 Release Support should empower Children and Young People to have their views and wishes heard and their rights respected with regard to their continued care and their licence conditions under supervision of their Youth Offending Team or Probation Worker. Even where a Child or Young Person asks an Advocate to support them in discussions and/ or sessions with family members of other professionals, for example, the Supplier's role is to provide advocacy to and empower the Child or Young Person.

6.1.4 The Supplier will work to build relationships with those Children and Young People who are eligible for and who consent to engage with Release Support whilst they are still in the Secure Establishment, prior to release.

6.1.5 Children and Young People eligible for Release Support are those serving a custodial sentence with a period of custody (remaining) that is at least 12 weeks in length to their calculated release date. The Authority will provide the Supplier with reasonable notice, of at least 12 weeks, prior to Children and Young Peoples' release dates.

6.1.6 Release Support should be flexible and tailored to the individual Child or Young Person and available for up to 12 weeks post-release with the possibility of an extension to meet the individual needs of the Child or Young Person in exceptional circumstances.

6.1.7 The Supplier can engage eligible Children and Young People about Release Support via any means available to the Service, and informed by the Child or Young Person's views and wishes – physical, digital, telephone contact, etc.

6.1.8 For those Children and Young People who are eligible and wish to access this support, the Supplier Staff should agree a Post-Release Advocacy Plan with the Child or Young Person so that they understand and have a documented record of the support and help they have agreed that the Services will provide. This should be regularly reviewed in partnership with the Child or Young Person, particularly regarding the disengagement of Advocates at the agreed point/ duration.

6.1.9 The Supplier shall for this Release Support service use effective working arrangements with the Secure Establishment Resettlement Practitioner / case work team – and reflected Local Protocols (See Section 4 of this Specification) – to support those Children and Young People whom the Supplier is working with.

6.1.10 The Supplier shall work effectively and constructively with individual Secure Establishments and the Authority to establish effective communication methods around the Release Support Optional Service, including, but not limited to:

a) Notification of Children and Young Peoples' calculated date of release from the Secure Establishment, and their location within the Secure Establishment;

b) Providing information to Children and Young People and Secure Establishment staff outlining the service and eligibility.

6.1.11 Just as the Supplier is required to work collaboratively with Secure Establishments whilst Children and Young People are in youth custody, the Supplier should in delivering Release Support work to build trust with the Child or Young Person's family / carer as a vital means of support, even where the Child or Young Person is living away from their family.

6.1.12 The Supplier will also build positive relationships with stakeholders and agencies key to supporting and resolving the Child or Young Person's concerns. This is likely to include working collaboratively across a wide range of issues, from immediate practical concerns – such as housing, finance, or attending appointments – through to longstanding social, emotional and wellbeing issues – which may include engaging the relevant statutory providers for support a Child or Young Person is entitled to.

6.1.13 The Supplier's Staff should take care not to duplicate the roles and responsibilities of external parties and statutory providers in providing Release Support to Children and Young People in their communities.

6.1.14 The Supplier shall work with each Secure Establishment and key stakeholders to ensure that the role of the Release Support service is understood. This may include, but not be limited to:

a) Meeting with staff within the Secure Establishment and providing briefings or information as required, outlining the service;

b) Offer briefing sessions related to the service to Children's YOT or Young People's Probations workers, and families /carers;

c) Being clear with Children and Young People, their families / careers and key stakeholders about the maximum duration of Release Support available to them.

6.2 Follow-On Interviews

6.2.1 This Follow-On Interview optional service is to provide Children and Young People with an opportunity to give their views, feedback, and feelings about their lived experience in the Secure Establishment(s) – including on their safety and wellbeing – and following their release or movement out from that Secure Establishment.

6.2.2 Children and Young People will see that this optional service is an independent consultation and meaningful engagement with them, to reflect upon their time in youth custody and the key concerns facing them in continuing to build a positive future.

6.2.3 Children and Young People who are engaged with the Supplier Release Support services are eligible also for Follow-on Interviews, as are those who transition to (adult) custody. The Supplier should look to integrate Follow-On Interview with Release Support optional services, so that Children and Young People eligible for both receive a continuous and consistent service from Supplier staff.

6.2.4 The Supplier staff will gain informed consent from Children and Young People to engage them in their communities, or in youth/ adult custody after they leave the Secure Establishment (YOI/ STC) to conduct a Follow-on Interview. The Supplier must be clear with Children and

Young People that they are allowed the right to choose whether to engage with Follow-on Interviews and retain this right.

6.2.5 Follow-on Interviews will be planned for after the Child or Young Person leaves the Secure Establishment (Youth Custody). The interview can take place via a variety of methods, to suit the individual Child or Young Person, including (but not limited to) a face-to-face discussion or telephone conversation.

6.2.6 The Supplier will work with the Secure Establishment to ensure that the Child or Young Person, key professionals working with them (i.e. their YOT or probation worker if released to their local communities; and Offender Manager or similar if transitioned to adult custody) know that the Supplier will be contacting them following their release.

6.2.7 Once these Optional Services are activated, the Supplier will report to the Authority on trends and identifying key themes across the cohort and according to each Secure Establishment regarding both Release Support and Follow-on Interviews.

6.2.8 These optional services will also be in scope for monthly, quarterly and annual reporting requirements, as outlined in Section 5 of this Specification and Schedule 10 (Performance Mechanism).

6.2.9 As well as being used to manage these Optional Services, the Authority will look to share relevant information on Release Support and from Follow-on Interviews with key partners local to each Secure Establishment and of national significance to the Youth Justice System.

SOCIAL VALUE

Section 7 : Social value requirements

Outcomes
The Supplier tackles inequality in employment, skills and pay in the Contract workforce and has in place, measures, and processes for supporting in-work progression.
Service Requirements
The Public Services (Social Value) Act came into force on 31 January 2013. It requires people who commission public services to think about how they can also secure wider social, economic, and environmental benefits. In June 2018, central government announced it would go further and explicitly evaluate social value when awarding most major contracts. Government departments will be expected to report on the social impact of their major contracts. The Authority requires the Supplier to deliver social value against the policy outcome of tackling workforce inequality. <u>7.1 Tackle inequality in employment, skills and pay in the Contract workforce</u> 7.1.1 The Supplier is required to demonstrate an understanding of the issues affecting inequality in employment, skills and pay in the market, industry or sector relevant to the Contract, and in the Supplier's own organisation and those of its key sub-contractors. 7.1.2 The Supplier is required to develop and implement measures to tackle inequality in employment, skills and pay in the Contract workforce. 7.1.3 The Supplier's proposals in this area will be evaluated as part of the tendering exercise and will then form part of this Contract. Illustrative examples include but are not limited to: a) Inclusive and accessible recruitment practices, and retention-focussed activities; b) Offering a range of quality opportunities with routes of progression if appropriate, e.g. T Level industry placements, students supported into higher level apprenticeships; c) Working conditions which promote an inclusive working environment and promote retention and progression; d) Demonstrating how working conditions promote an inclusive working environment and promote retention and progression; e) A time-bound action plan informed by monitoring to ensure employers have a workforce that proportionately reflects the diversity of the communities in which they operate, at every level; f) Including multiple women, or others with protected characteristics, in shortlists for recruitment and promotions;

g) Using skill-based assessment tasks in recruitment;
h) Using structured interviews for recruitment and promotions;
i) Introducing transparency to promotion, pay and reward processes;
j) Positive action schemes in place to address under-representation in certain pay grades;
k) Jobs at all levels open to flexible working from day one for all workers;
l) Collection and publication of retention rates, e.g. for pregnant women and new mothers, or for others with protected characteristics;
m) Regular equal pay audits conducted.

7.1.4 In delivering measures to tackle workforce inequality the Supplier will consider activities to also support in-work progression. This may include activities that demonstrate and describe the Supplier's existing or planned:

a) Understanding of in-work progression issues affecting the market, industry, or sector relevant to the Contract, and in the Supplier's own organisation and those of its key sub-contractors;
b) Inclusive and accessible development practices, including those provided in the Guide for line managers: Recruiting, managing and developing people with a disability or health condition - GOV.UK (www.gov.uk);
c) Measures to support in-work progression to help people in the Contract workforce, to move into higher paid work by developing new skills relevant to the Contract.

7.2 Reporting Requirements for social value

7.2.1 The Supplier activities relating to tackling workforce inequality will be subject to data collection and reporting. The precise nature of the reporting and any related performance targets will be developed depending on the Suppliers proposed initiatives. However, the Supplier shall include in the Monthly Data Returns, Quarterly Contract Management Reports and the Annual Report, information on its performance against the social value requirements. Illustrative examples include but are not limited to:

a) Total percentage of full-time equivalent (FTE) people from groups under-represented in the workforce employed under the Contract, as a proportion of the total FTE Contract workforce, by UK region;
b) Number of full-time equivalent (FTE) people from groups under-represented in the workforce employed under the Contract, by UK region;
c) Total percentage of people from groups underrepresented in the workforce on apprenticeship schemes (Level 2, 3, and 4+) under the Contract, as a proportion of all the people on apprenticeship schemes (Level 2, 3, and 4+) within the Contract workforce, by UK region;
d) Number of people from groups under-represented in the workforce on apprenticeship schemes (Level 2, 3, and 4+) under the Contract, by UK region;
e) Total percentage of people from groups underrepresented in the workforce on other training schemes (Level 2, 3, and 4+) under the Contract, as a proportion of all the people on other training schemes (Level 2, 3, and 4+) within the Contract workforce, by UK region;
f) Number of people from groups under-represented in the workforce on other training schemes (Level 2, 3, and 4+) under the Contract, by UK region;
g) Percentage of all companies in the supply chain under the Contract to have committed to the five foundational principles of good work;

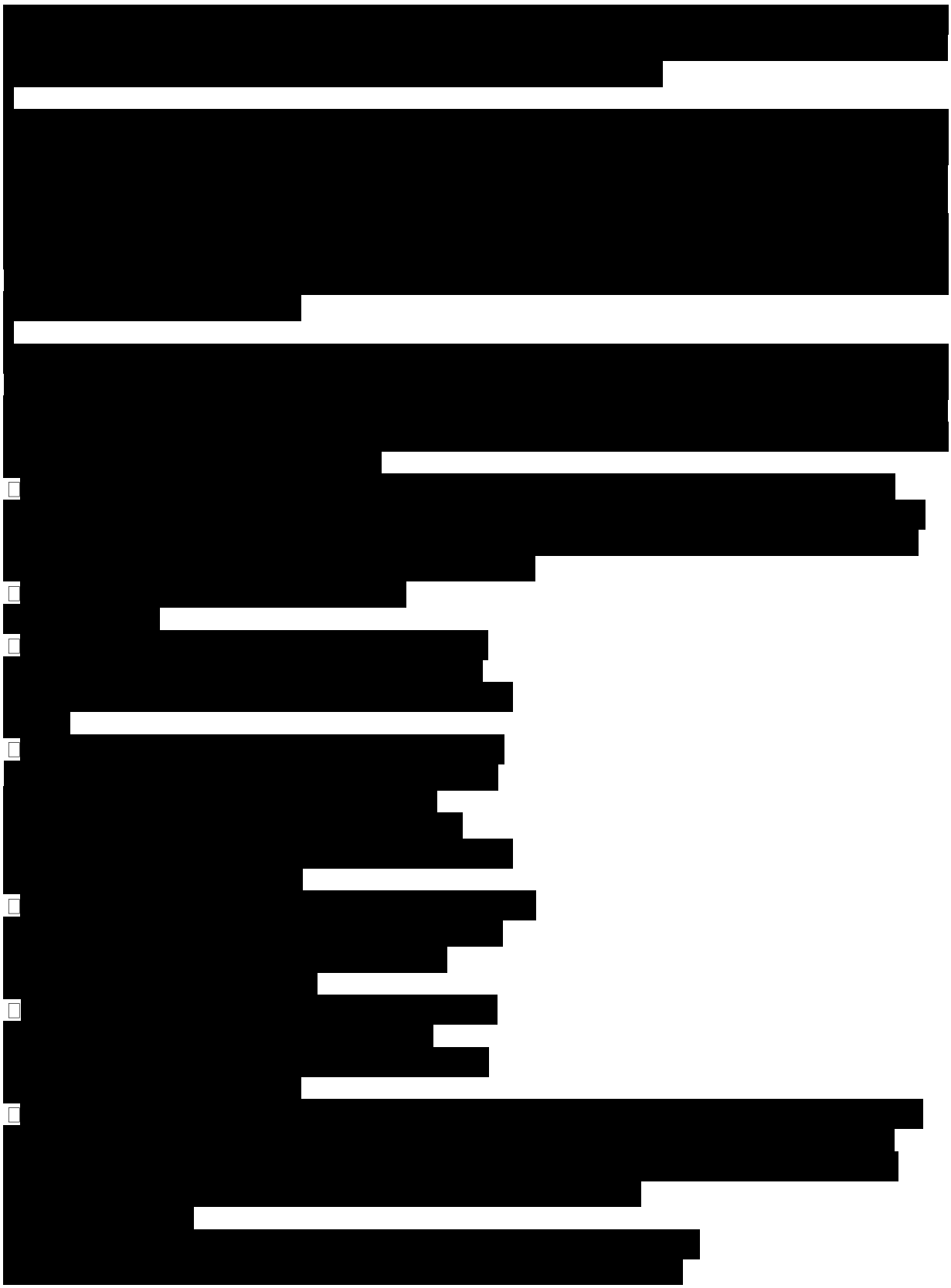
h) Number of companies in the supply chain under the Contract to have committed to the five foundational principles of good work.

ANNEX A: SUPPLIER PROPOSAL

Q1(a): Publicising the Services to Children and Young People.

[redacted]

Q1(b): Children and Young People are aware of the Service

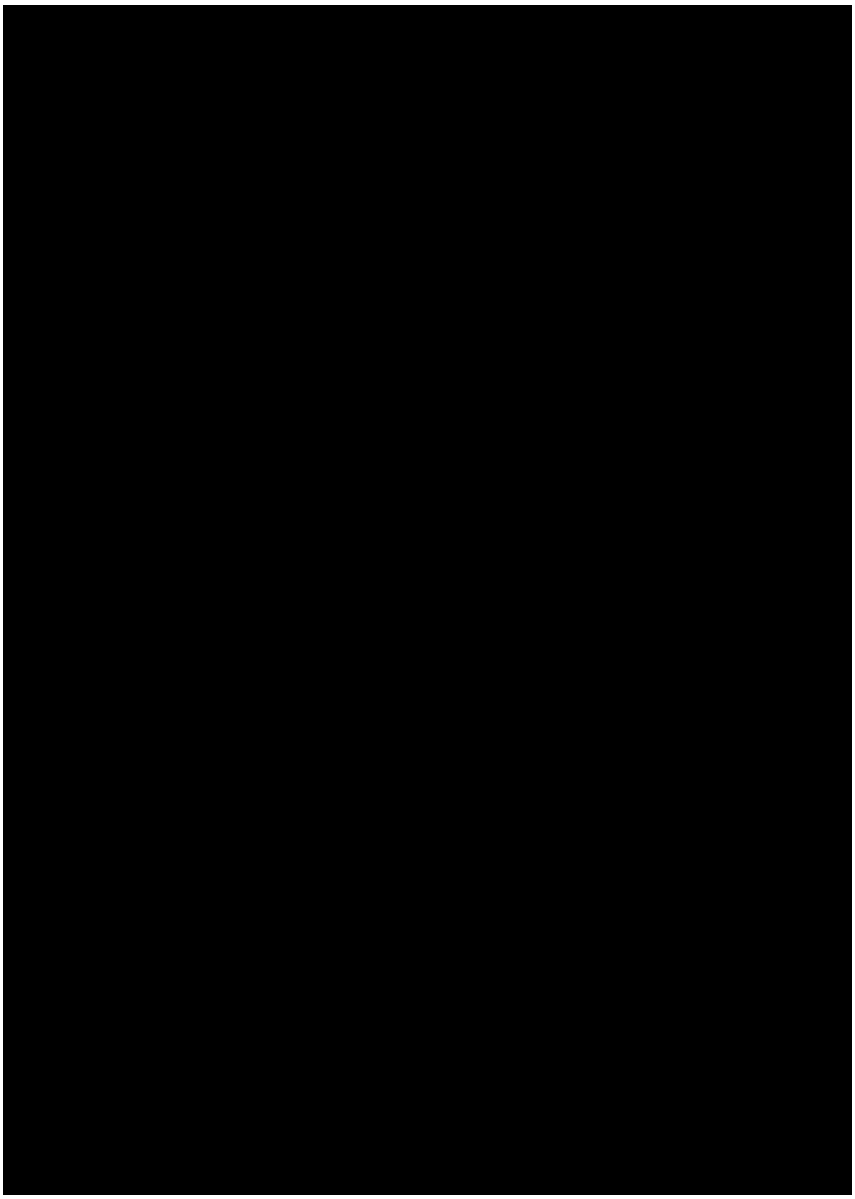


[redacted]

Q1**(c): Children and Young People are fully introduced to the Service**

[redacted]

Q1(d): Children and Young People's Rights Awareness -



[redacted]

Q1(e): Unit Visits

[redacted]

[redacted]

Q1(f) Referrals and Urgent Requests to Advocacy Services

[redacted]

[redacted]

Q1(g) Children and Young People's Councils/Forums

[redacted]

[redacted]

Q1(h) Children and Young People leaving the Secure Establishment

[redacted]

[redacted]

Q1(i): Safeguarding & Child Protection

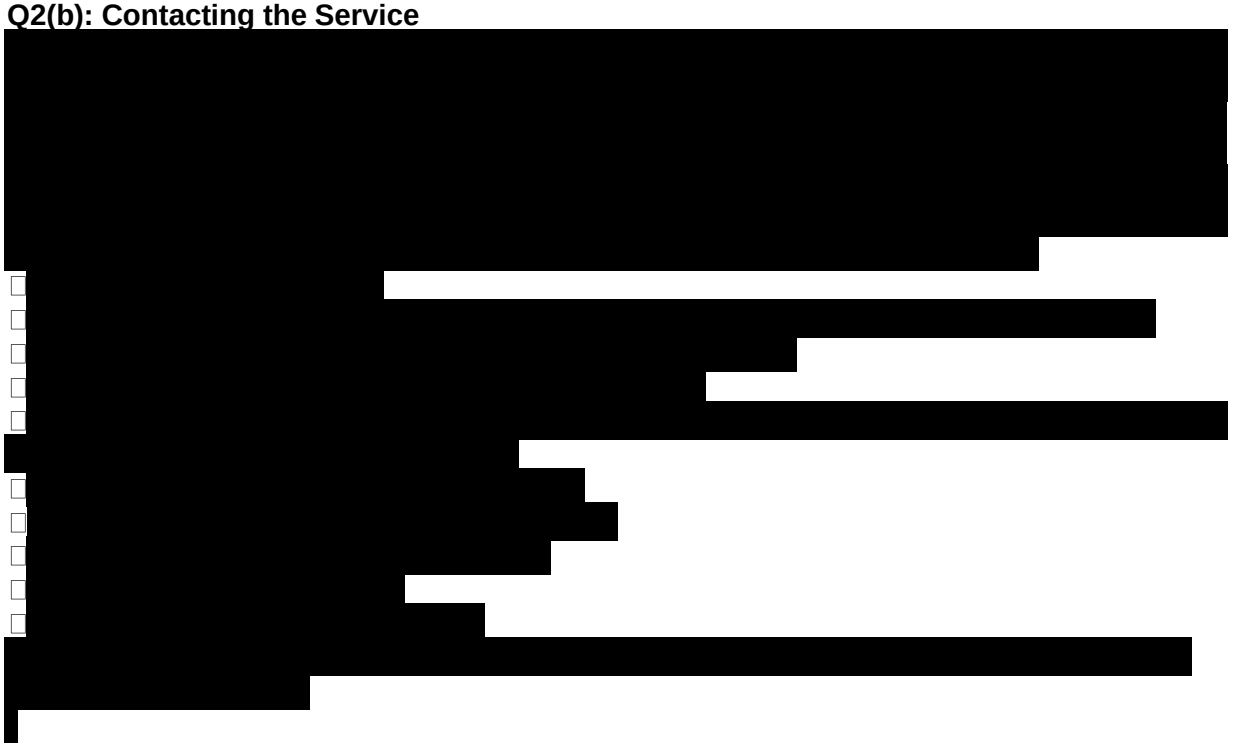
[redacted]

[redacted]

Q2(a): Working with Secure Establishments

[redacted]

Q2(b): Contacting the Service



[redacted]

Q2(c): Support during Secure Establishment Procedures

[redacted]

[redacted]

Q2(d): Raising awareness of the issues facing Children and Young People in custody

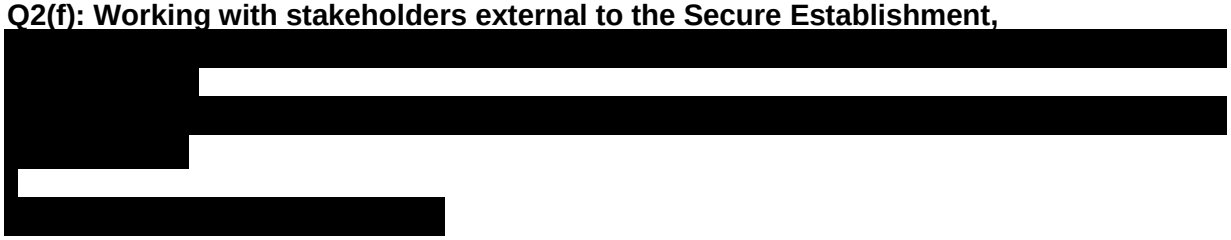
[redacted]

[redacted]

Q2(e): Working with Children & Young People's families / carers and significant others,

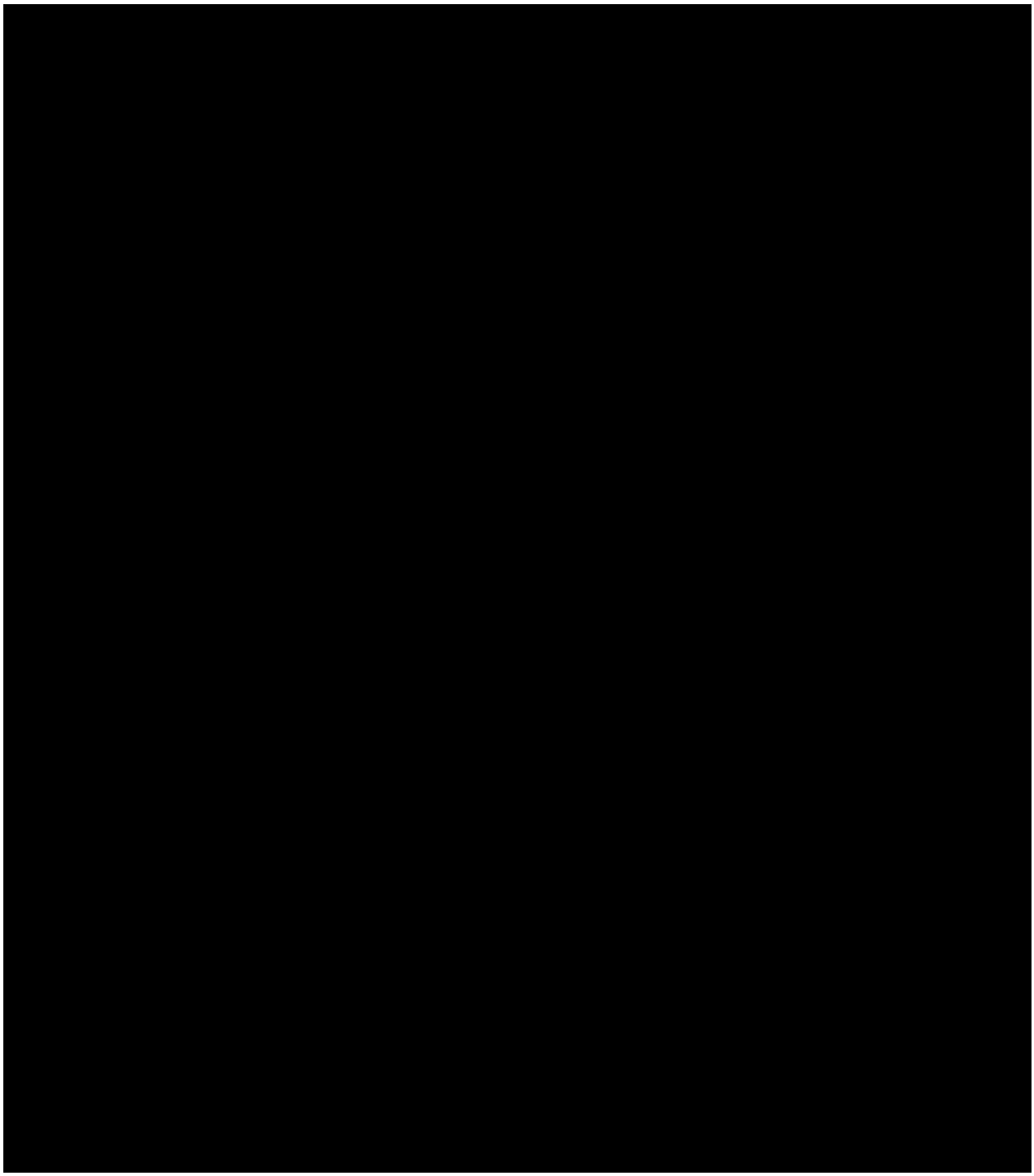
[redacted]

Q2(f): Working with stakeholders external to the Secure Establishment,



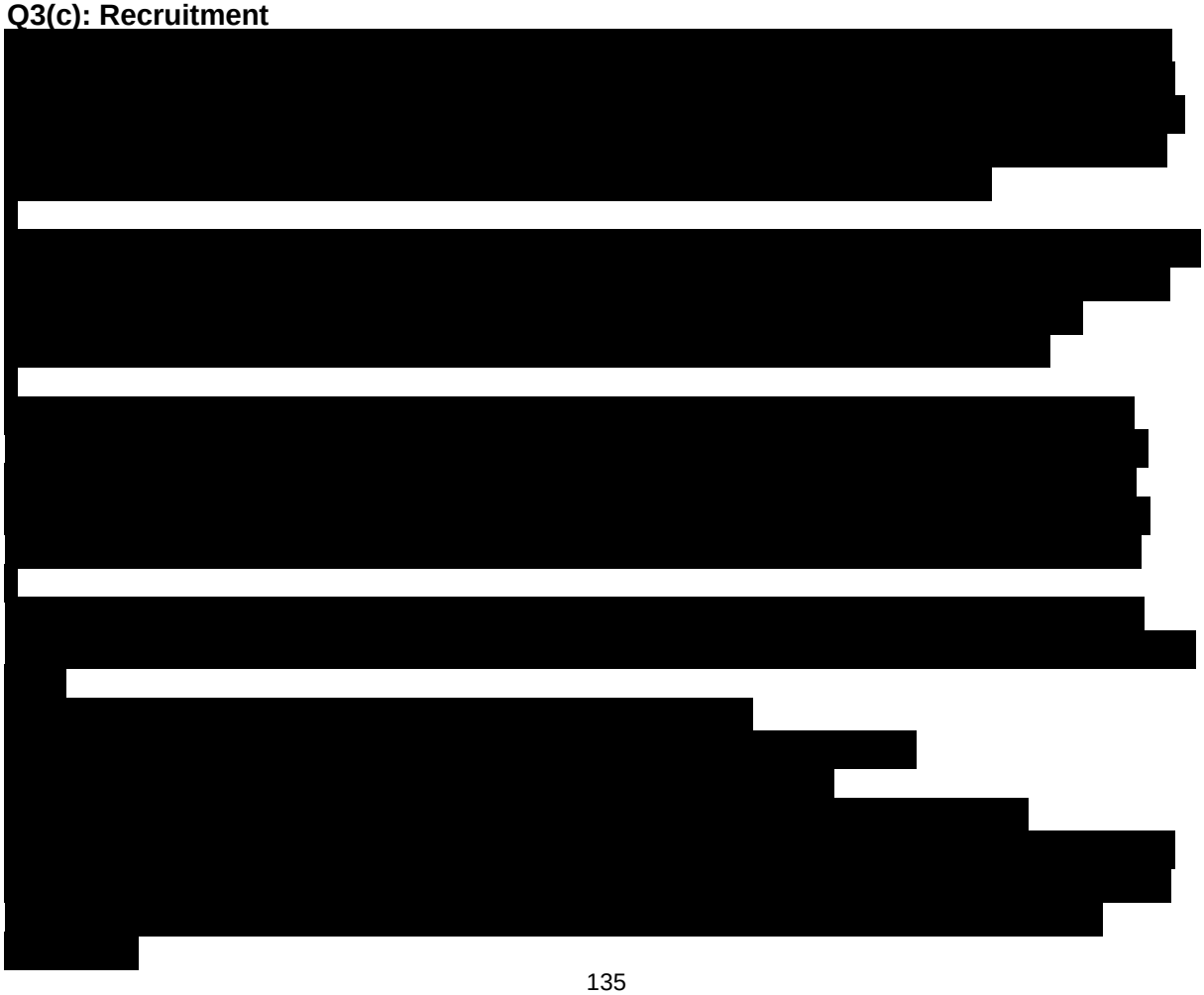
Q3(a) Local Protocols

Q3(b) Staff Solution



[redacted]

Q3(c): Recruitment



[redacted]

Q3(d): Staff Training

[redacted]

[redacted]

Q3(e): Management Structure and Staffing Processes, 250 words

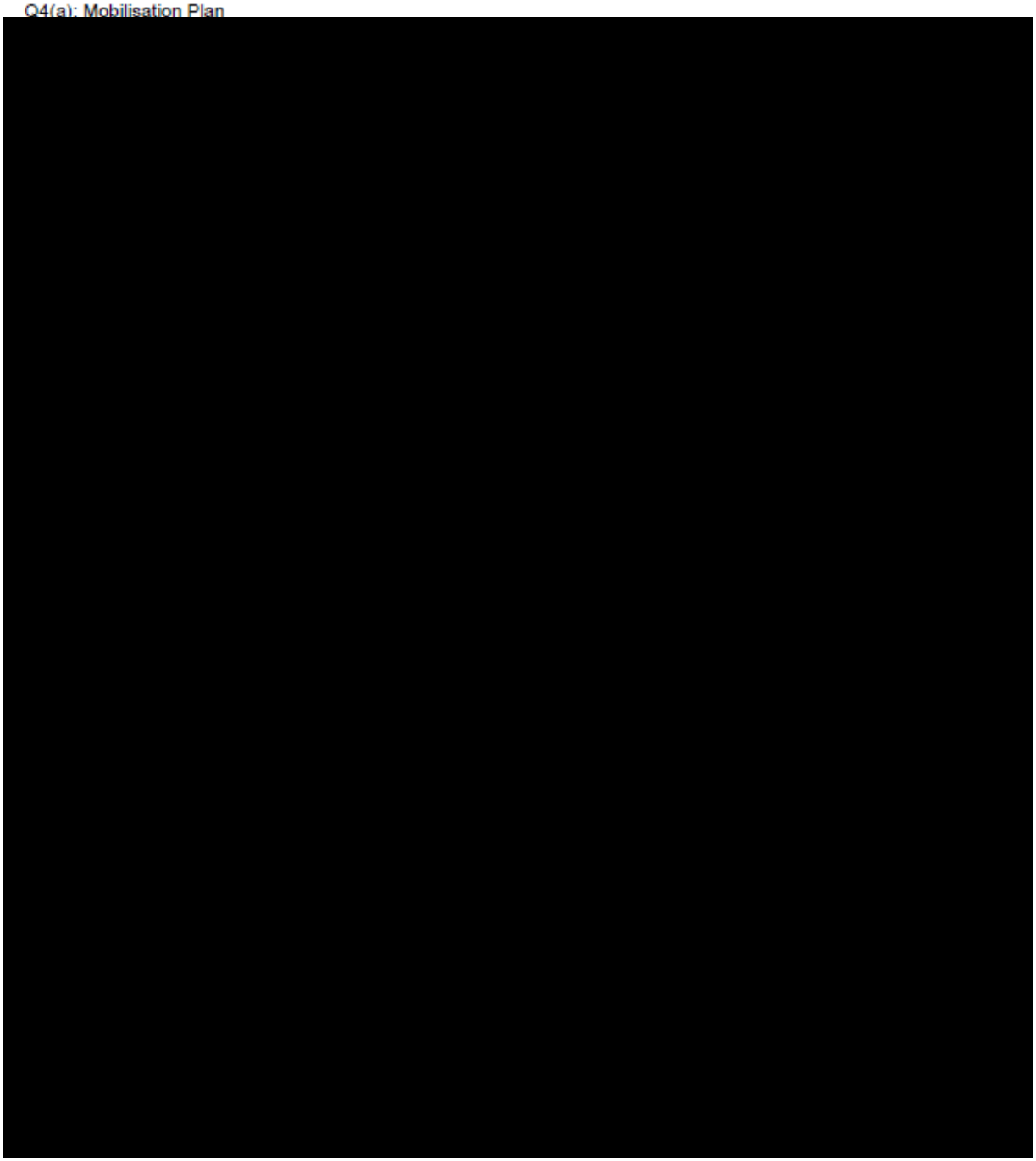
[redacted]

[redacted]

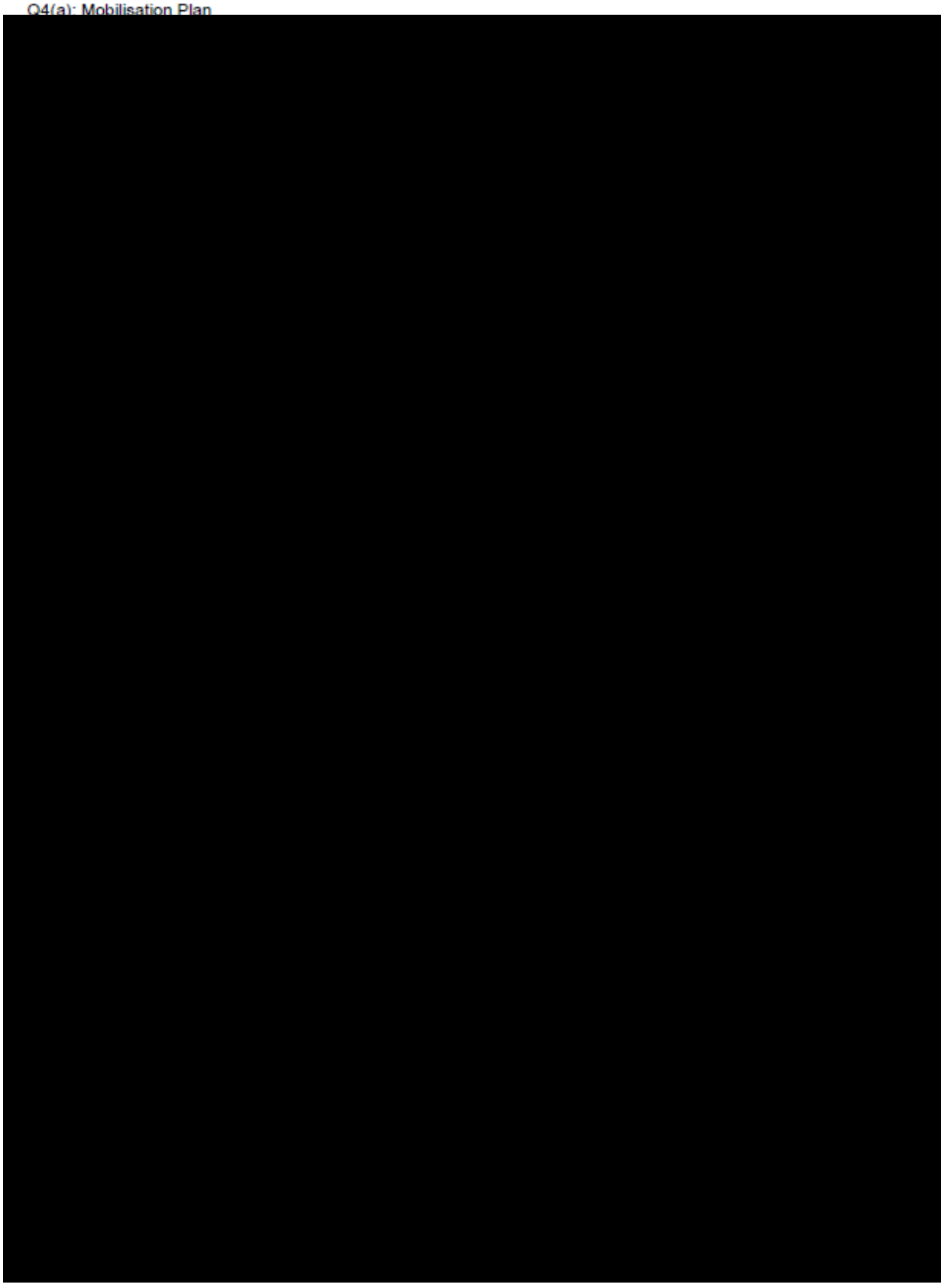
Q4(a): Mobilisation Plan

[redacted]

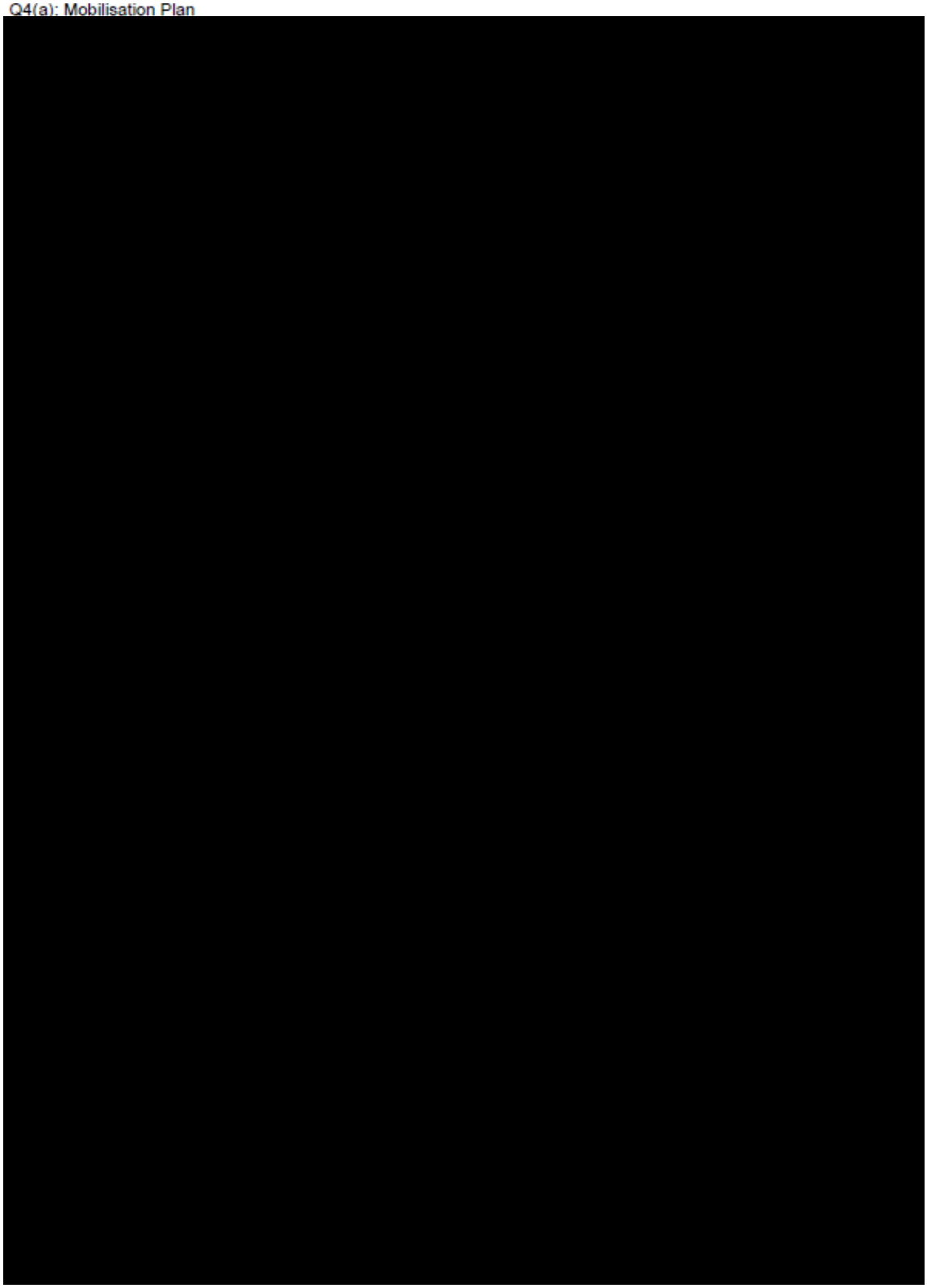
Q4(a): Mobilisation Plan



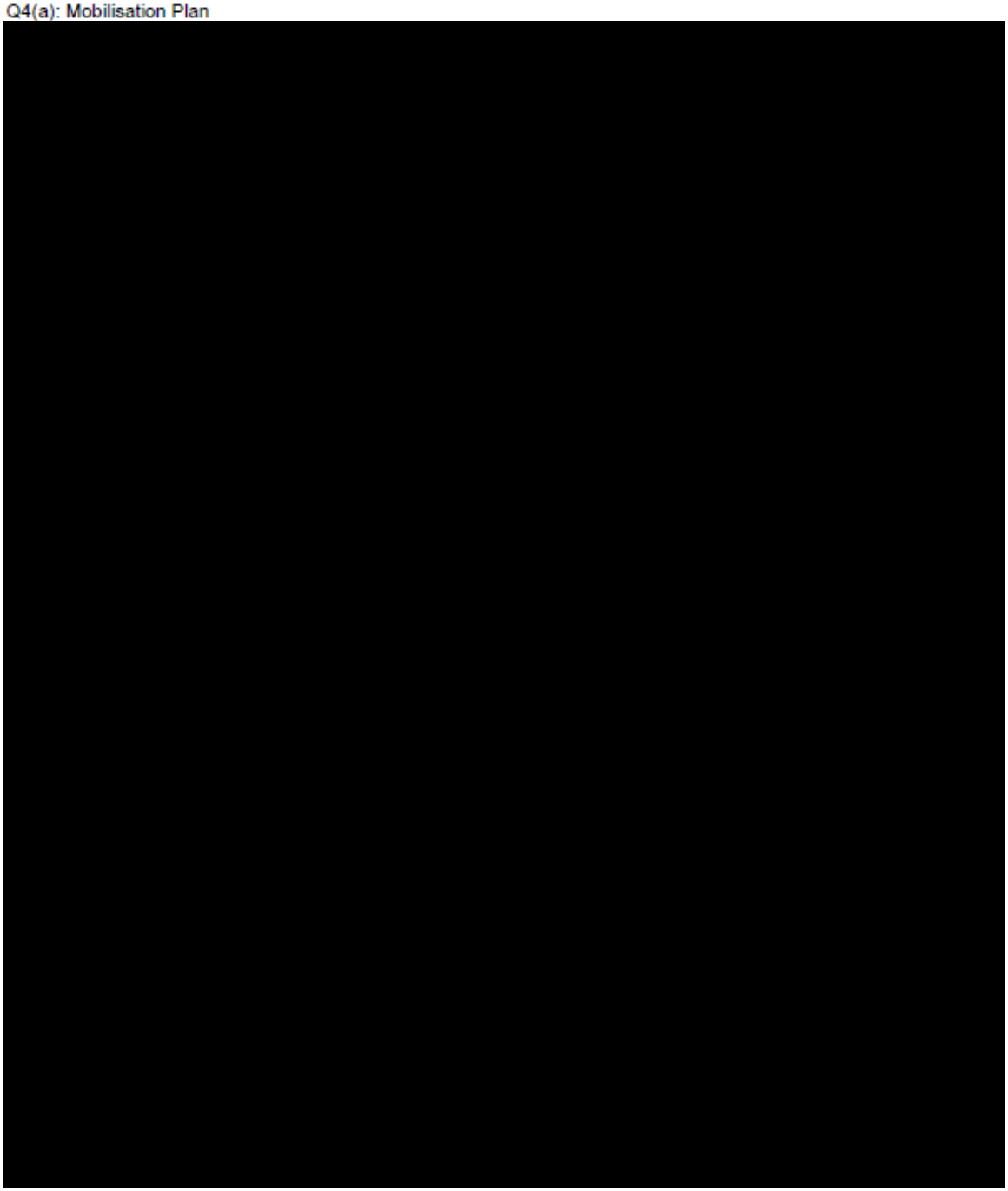
Q4(a): Mobilisation Plan



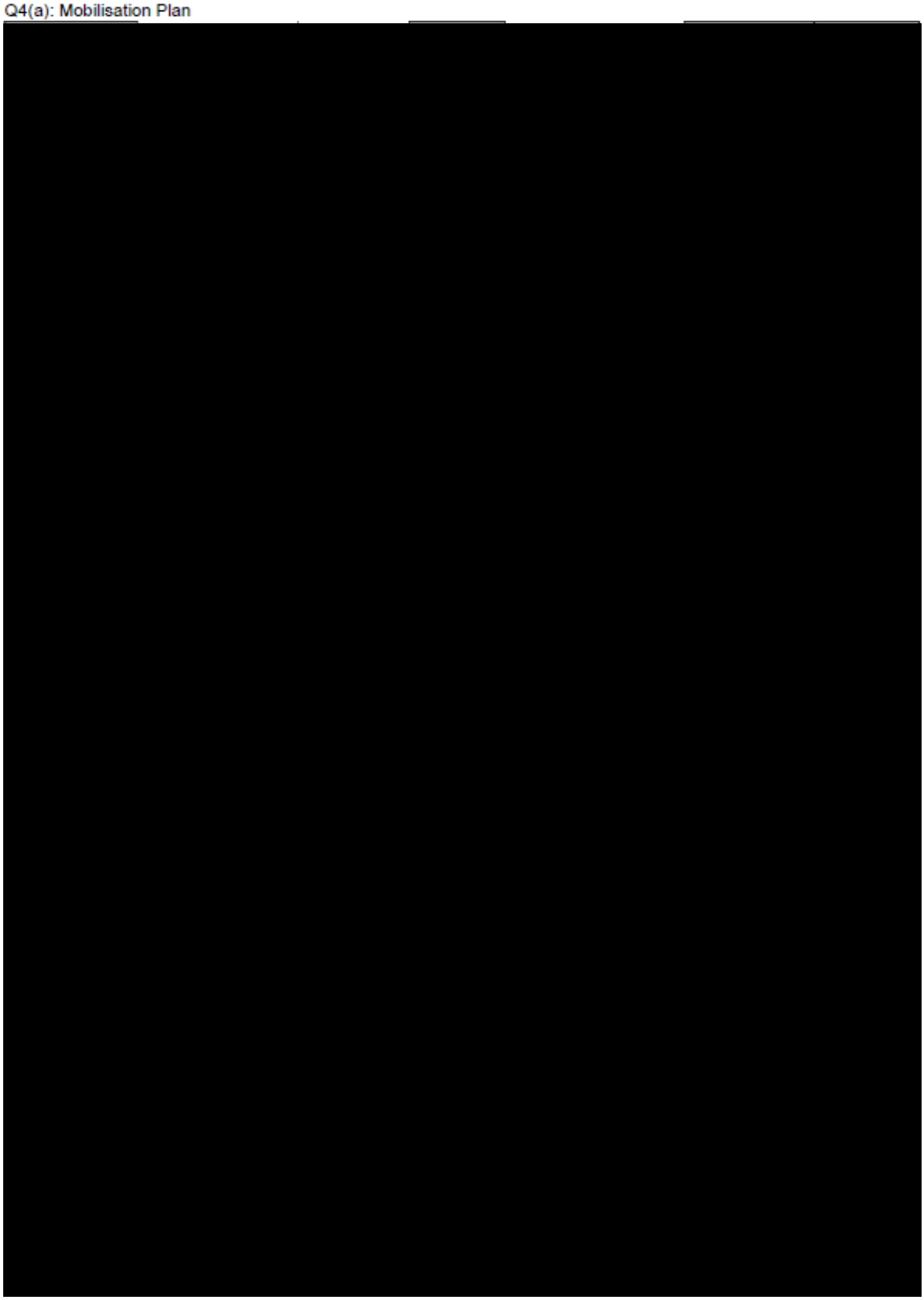
Q4(a): Mobilisation Plan



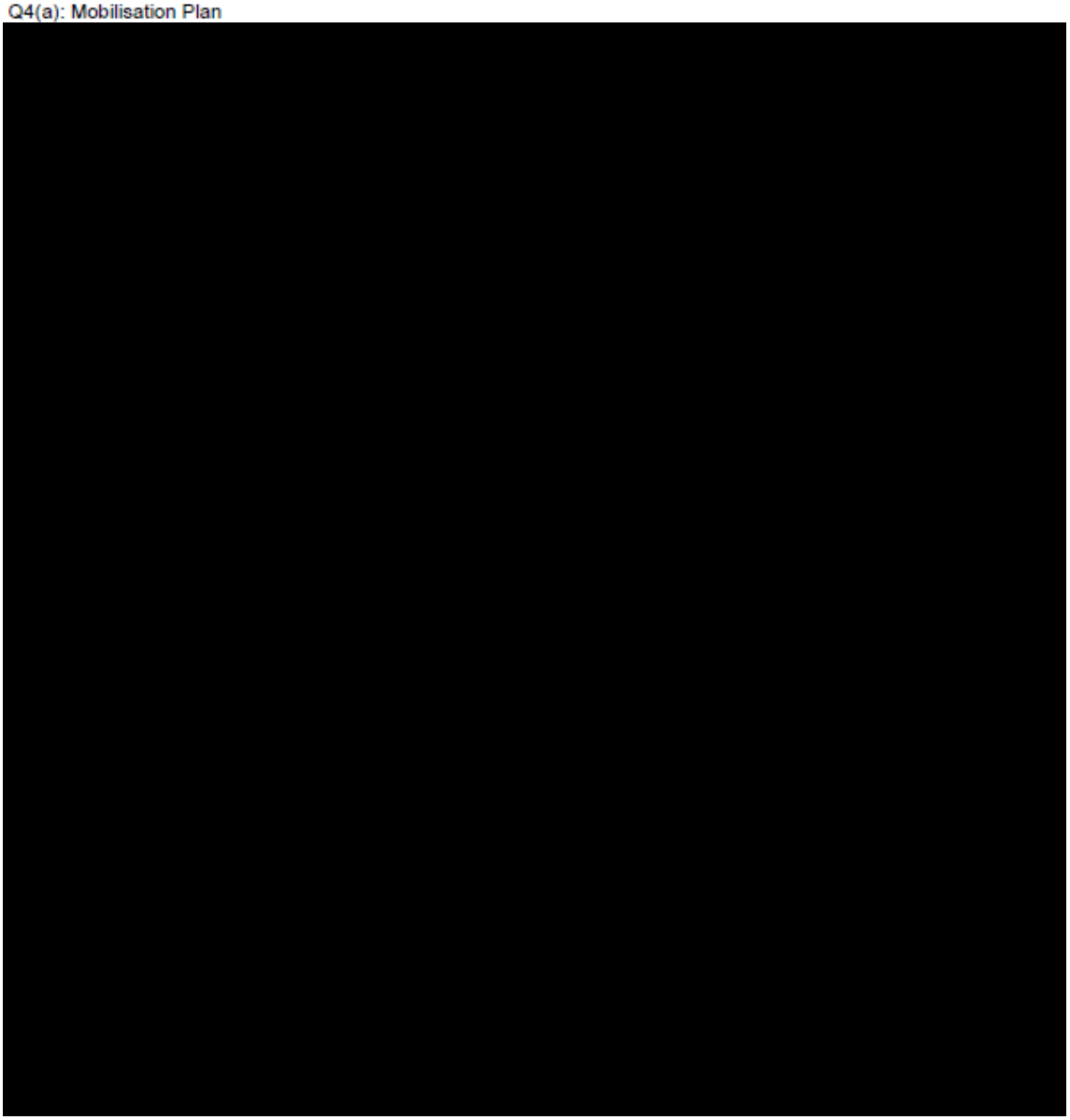
Q4(a): Mobilisation Plan



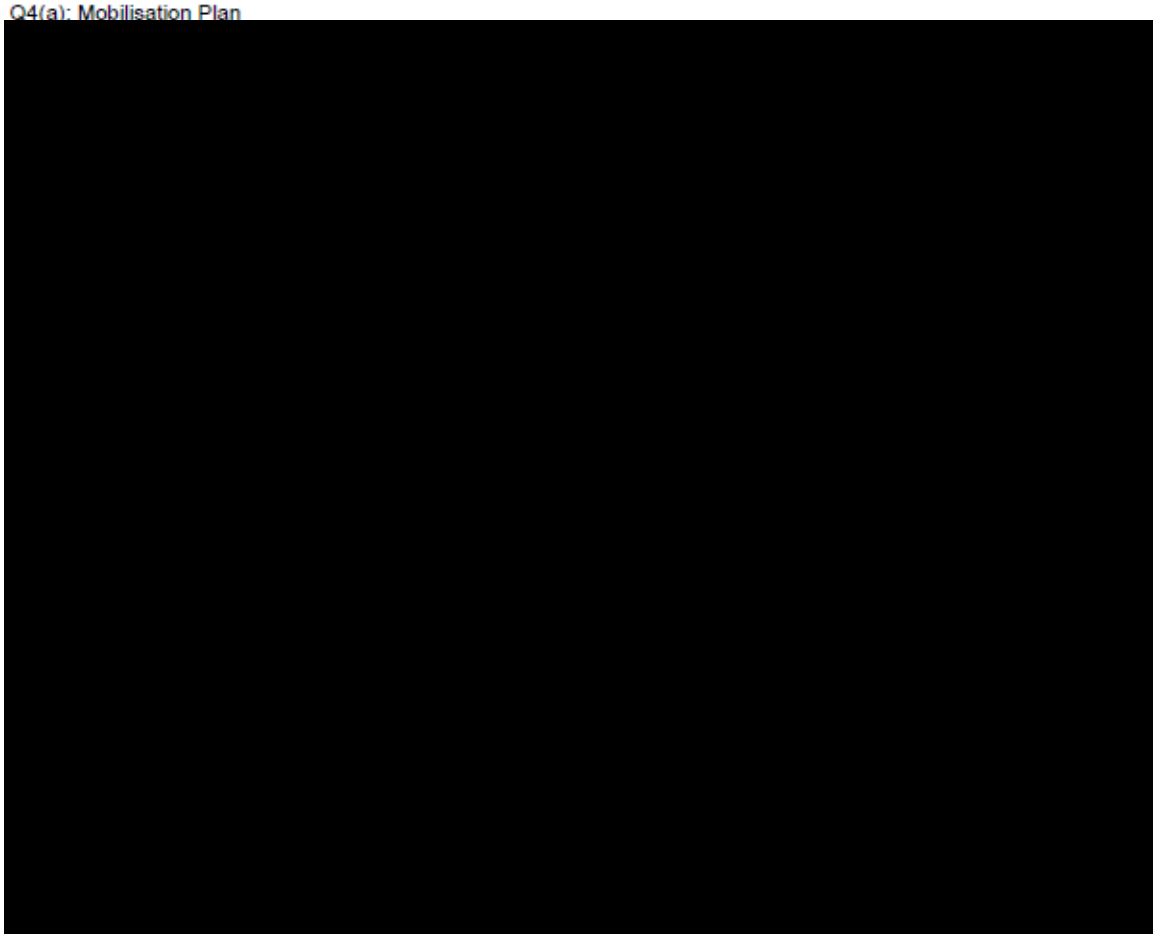
Q4(a): Mobilisation Plan



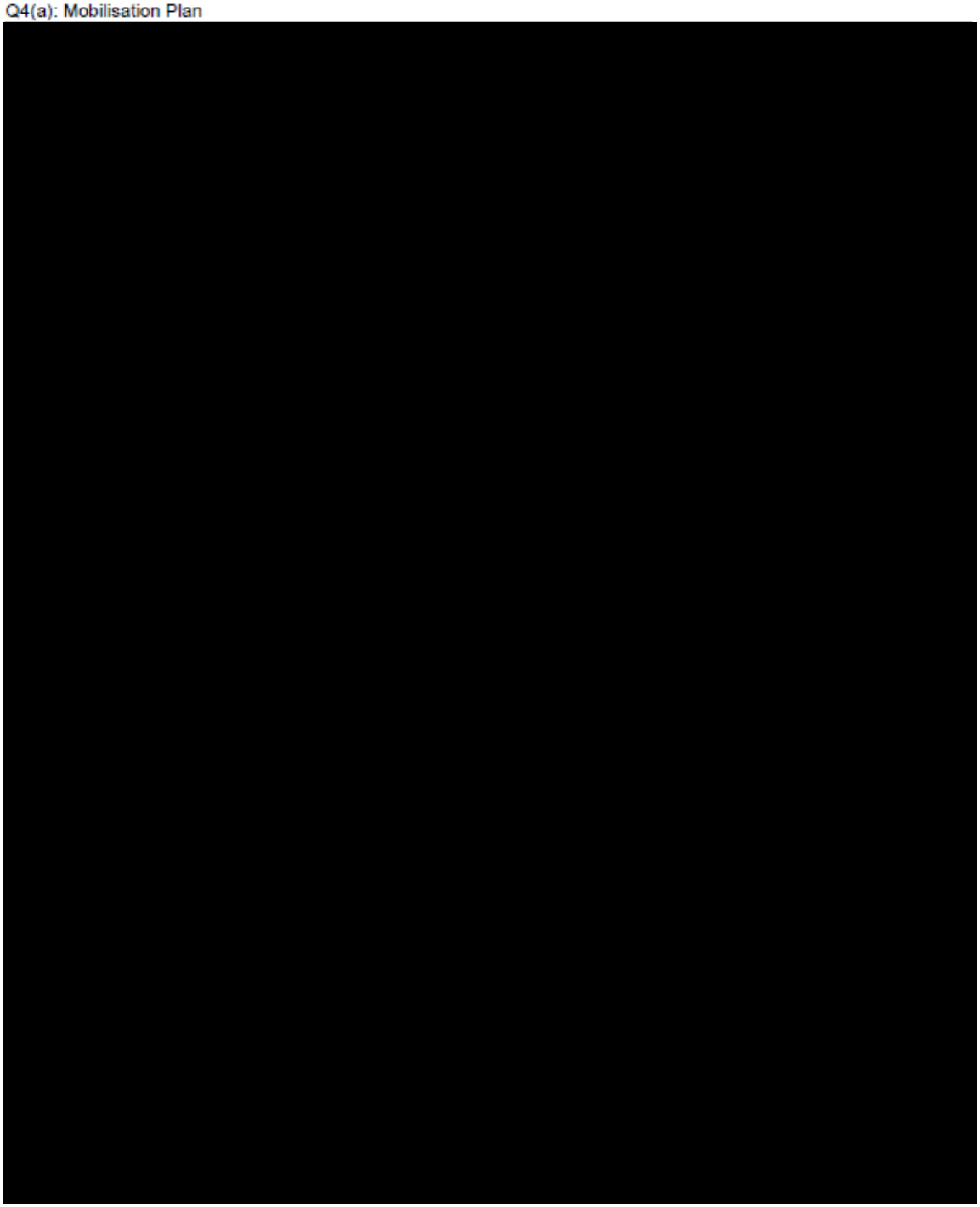
Q4(a): Mobilisation Plan



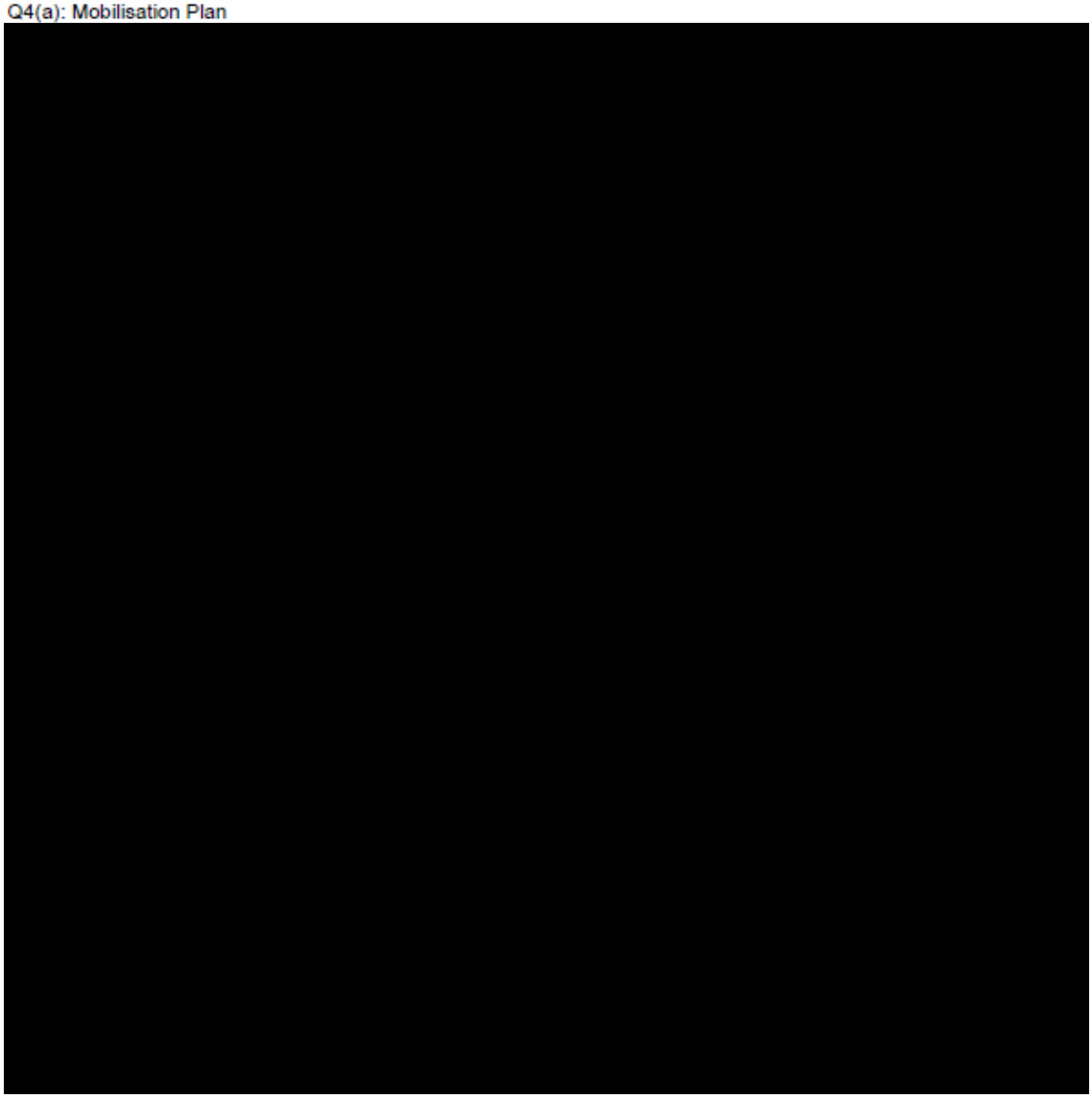
Q4(a): Mobilisation Plan



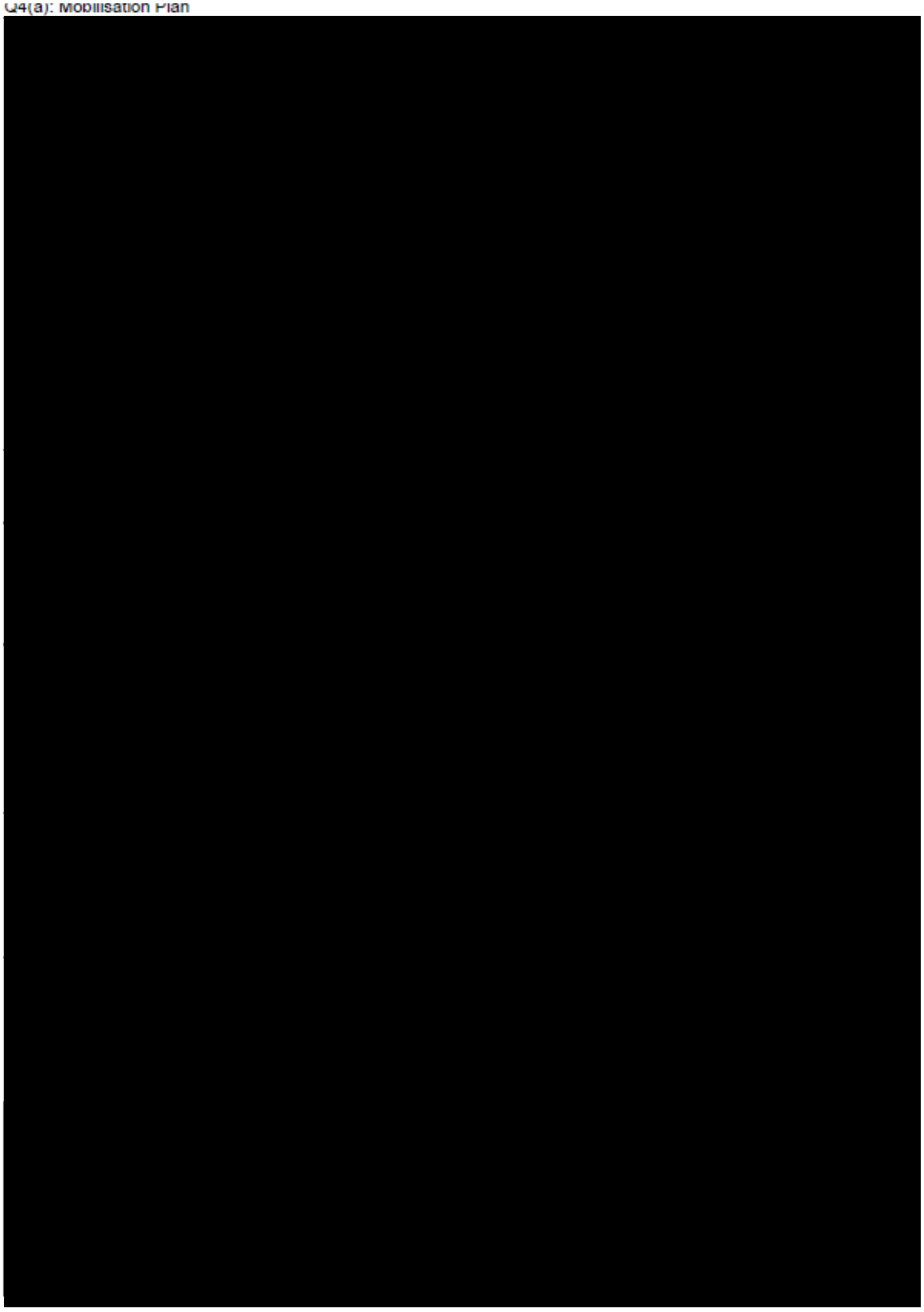
Q4(a): Mobilisation Plan



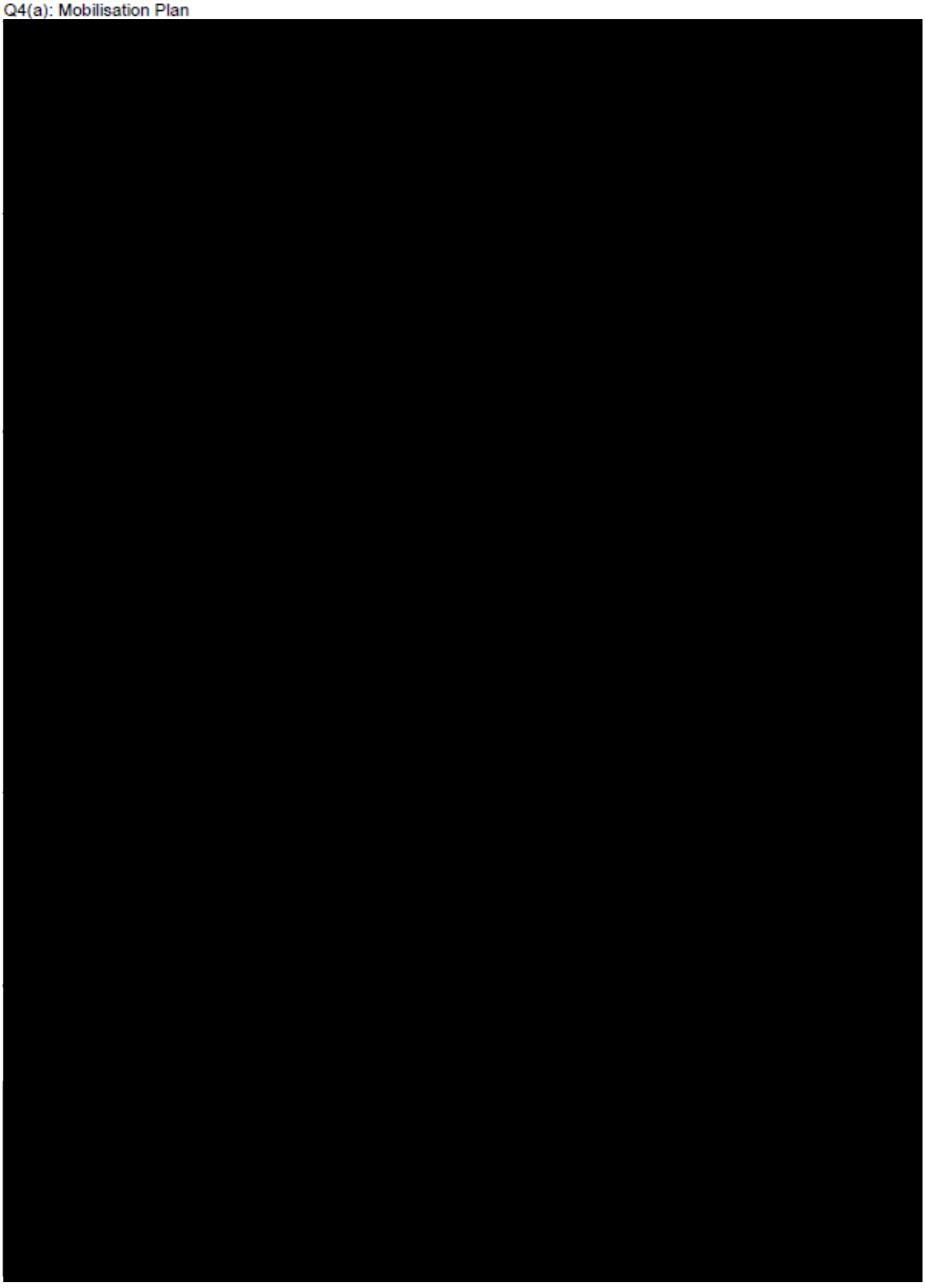
Q4(a): Mobilisation Plan



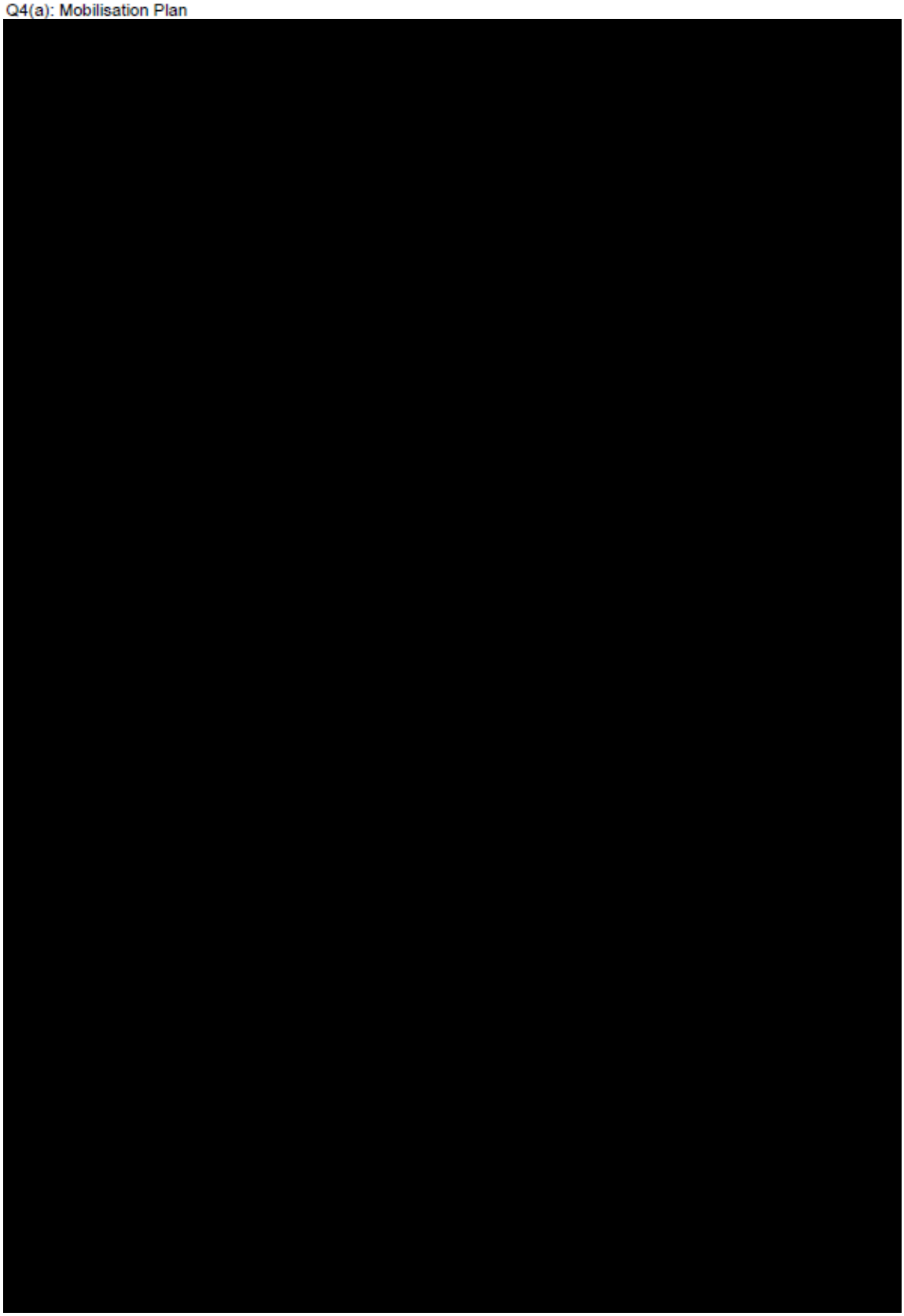
Q4(a): Mobilisation Plan



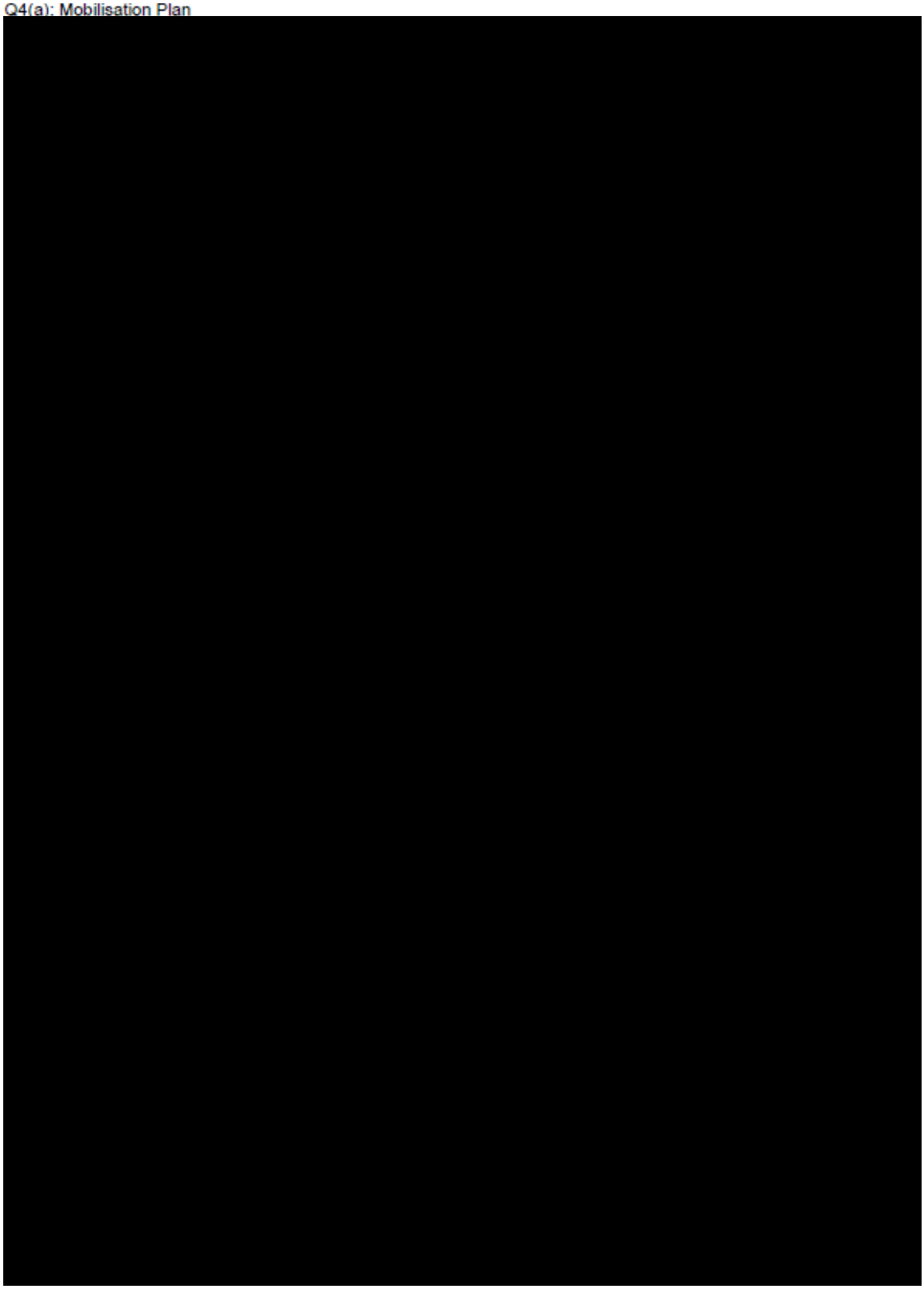
Q4(a): Mobilisation Plan



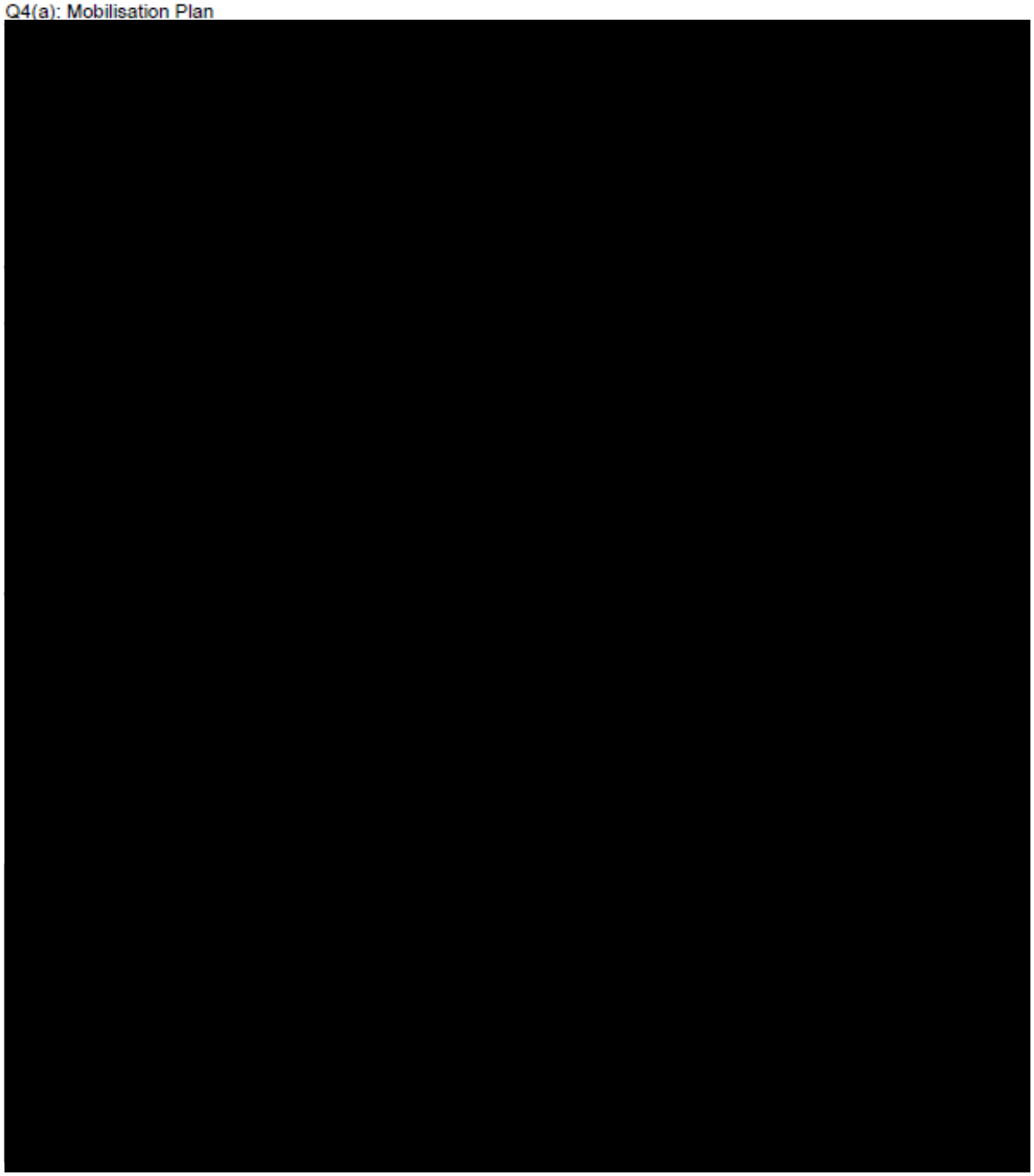
Q4(a): Mobilisation Plan



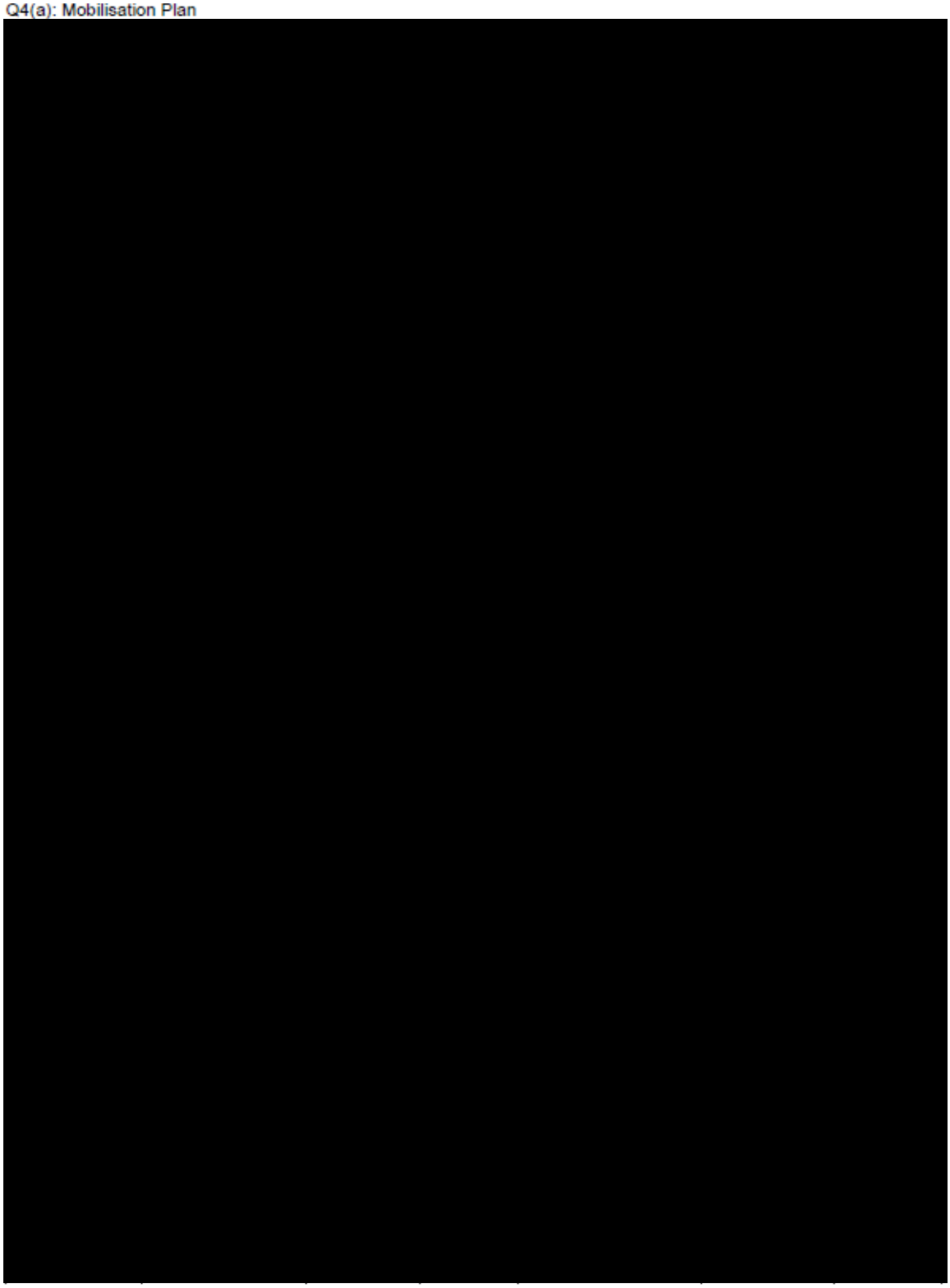
Q4(a): Mobilisation Plan



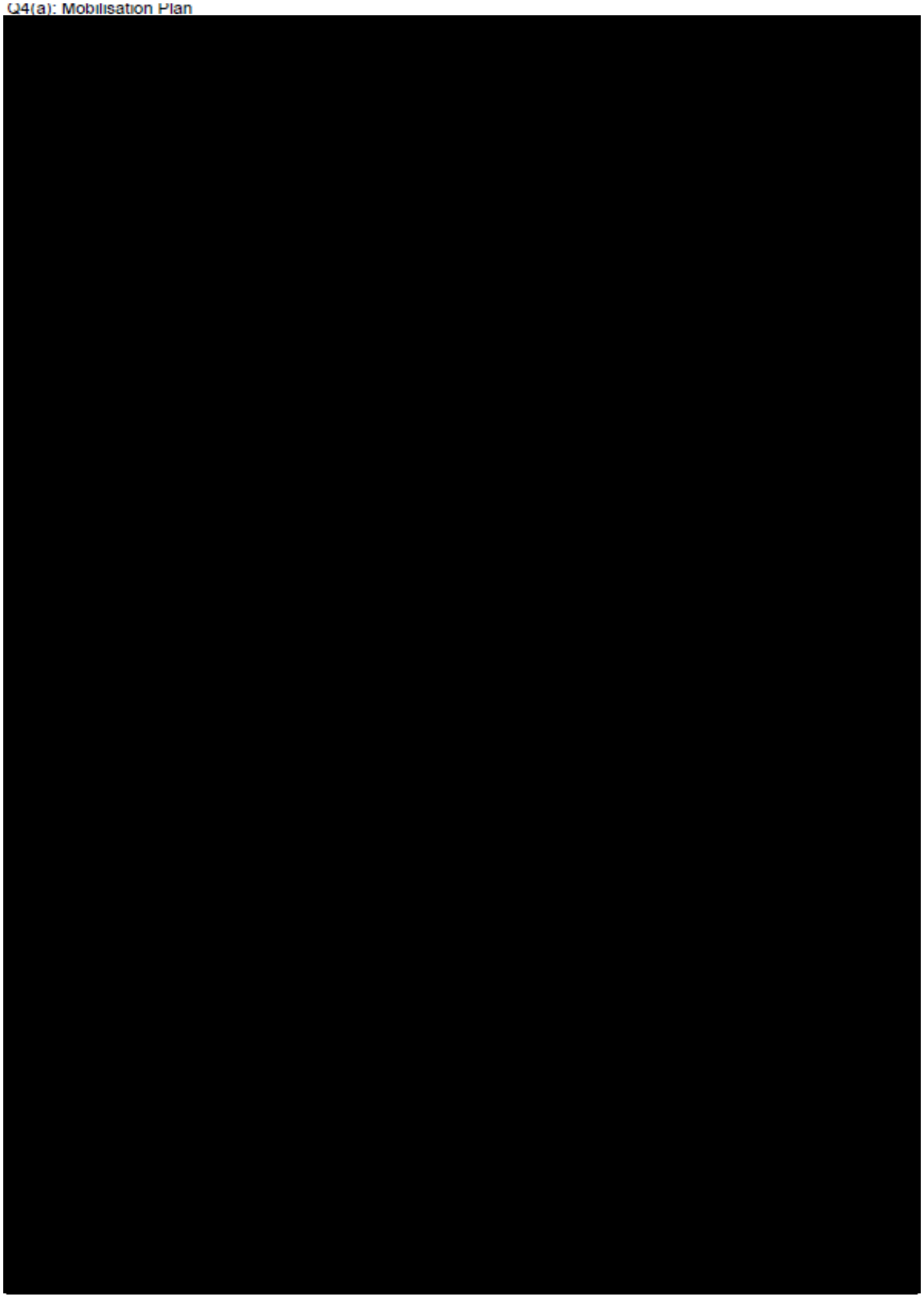
Q4(a): Mobilisation Plan



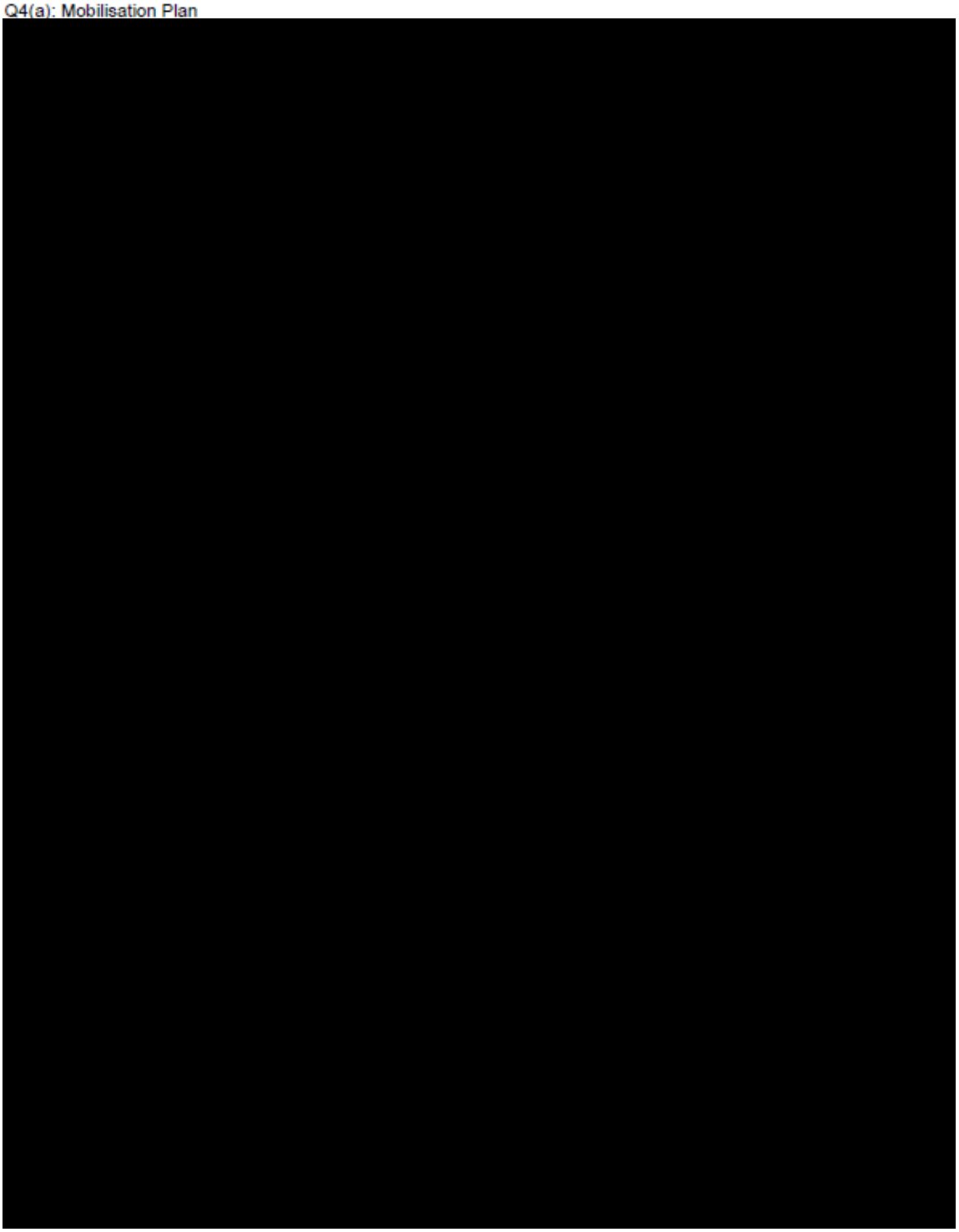
Q4(a): Mobilisation Plan



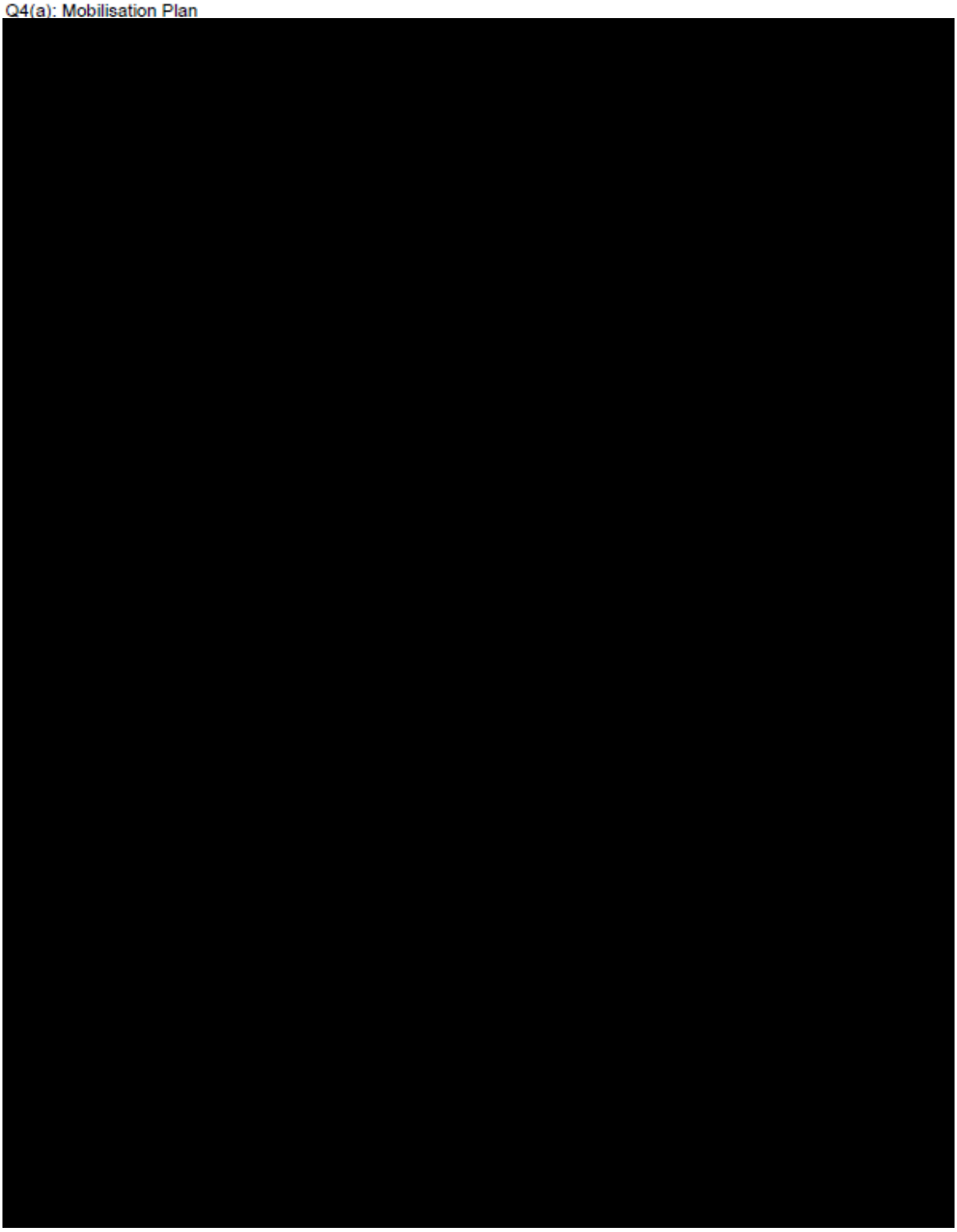
Q4(a): Mobilisation Plan



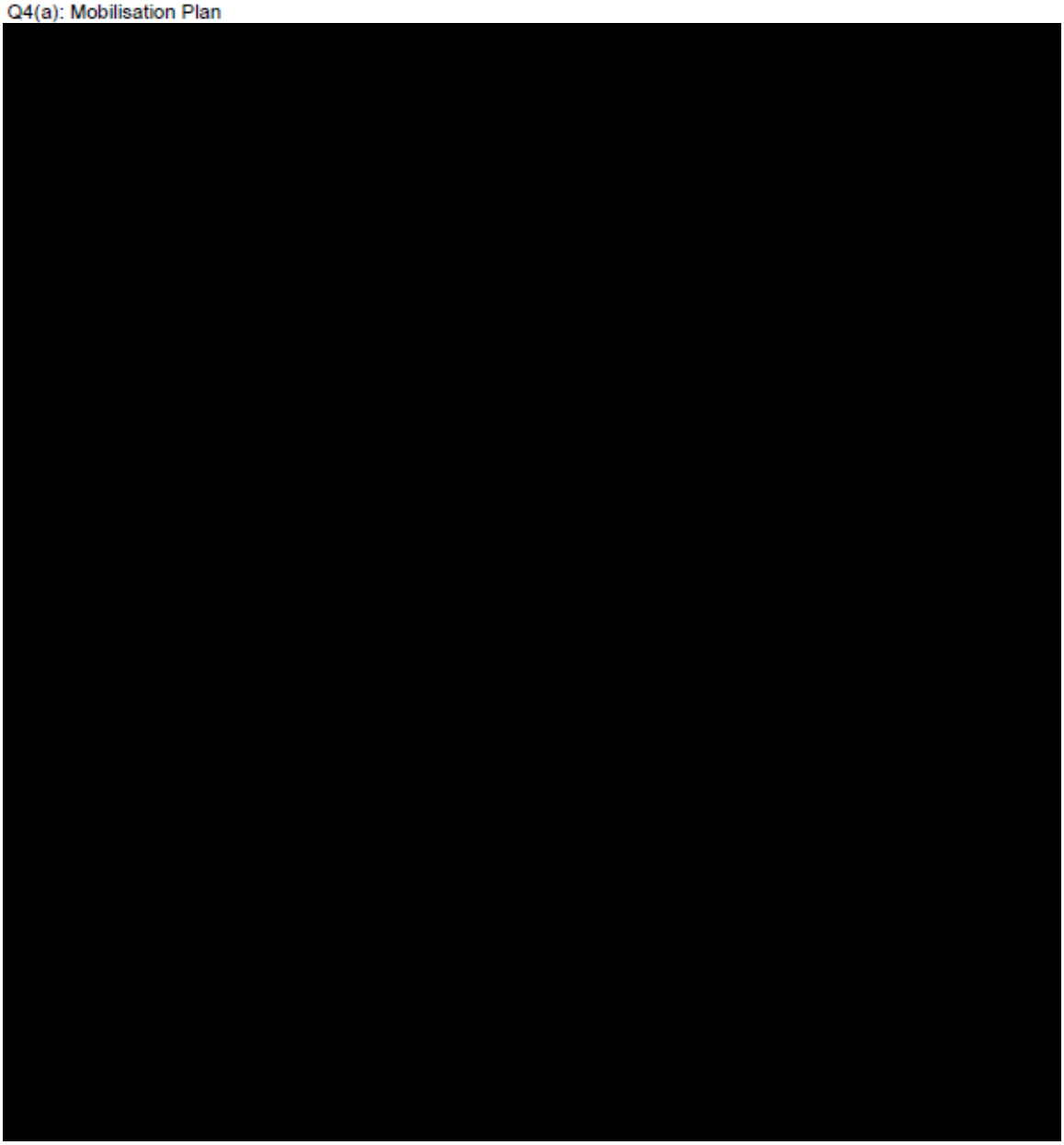
Q4(a): Mobilisation Plan



Q4(a): Mobilisation Plan



Q4(a): Mobilisation Plan



Q5(a): Electronic Case Management System, 250 words

[redacted]

Q5(b): Complaints in relation to the Advocacy Service

[redacted]

[redacted]

Q5(c): Reports and Delivery Plans

[redacted]

[redacted]

Q5(d): Information Management

[redacted]

[redacted]

Q5(e): Quality Assurance

[redacted]

[redacted]

Q5(e): Quality Assurance

[redacted]

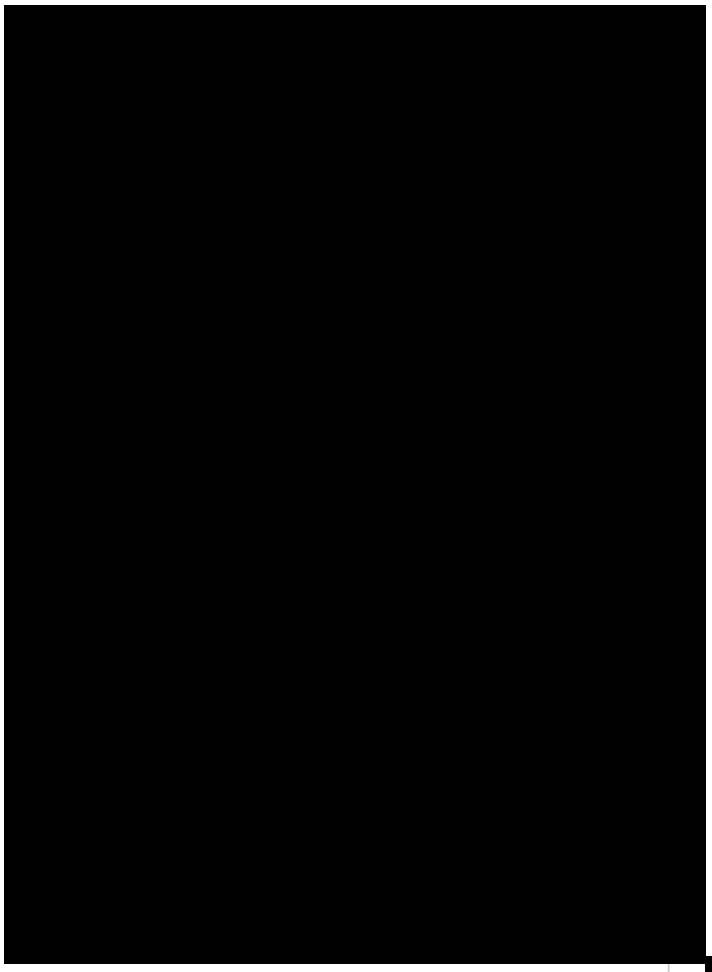
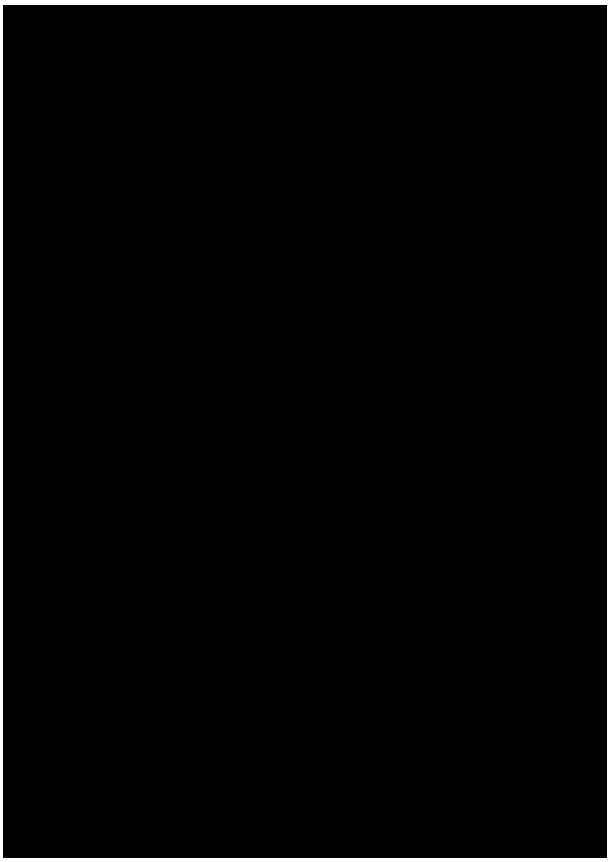
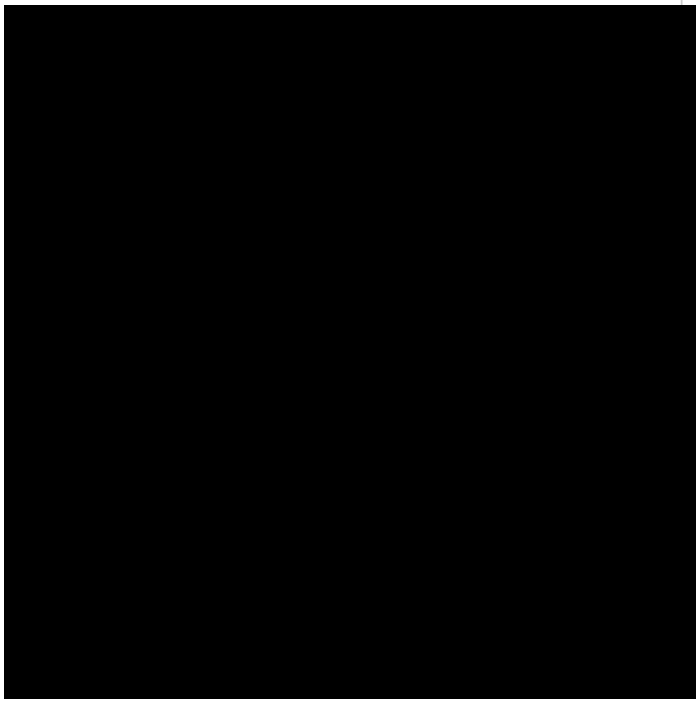
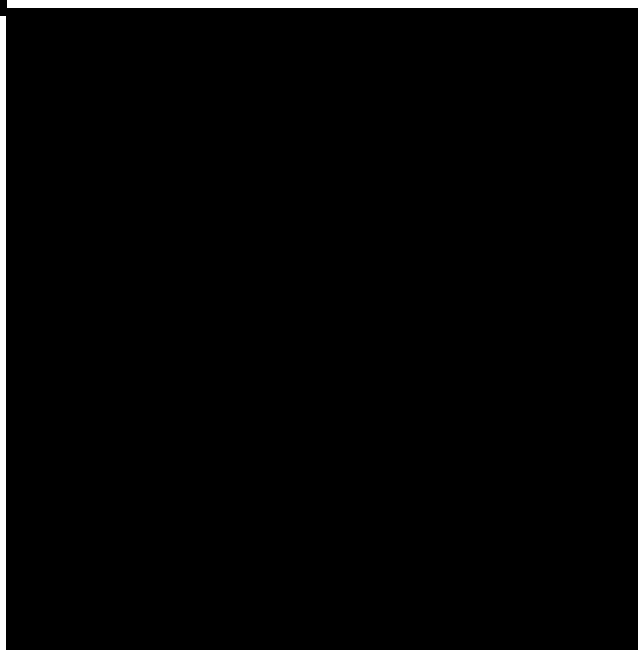
Q6(a): Social Value

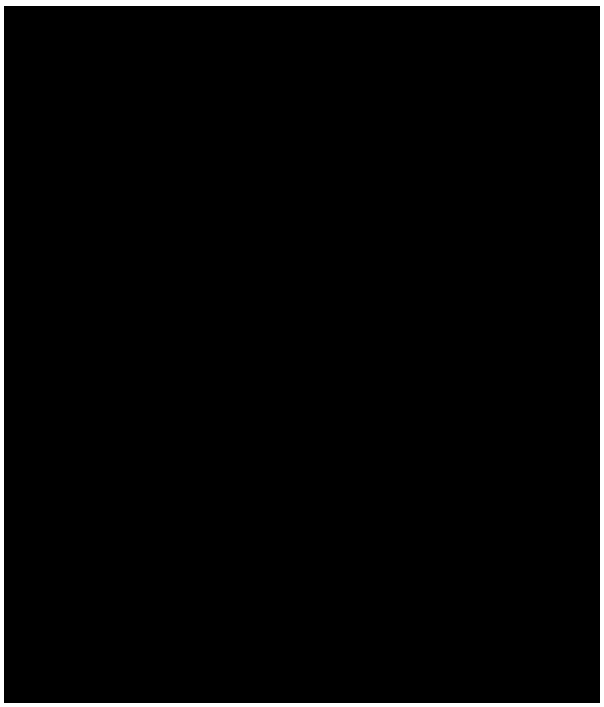
[redacted]

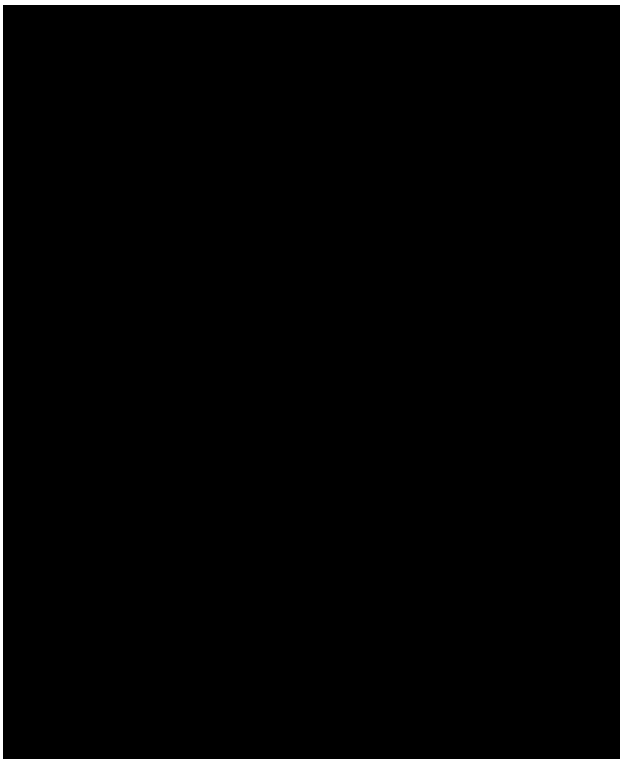
Q6(a): Social Value

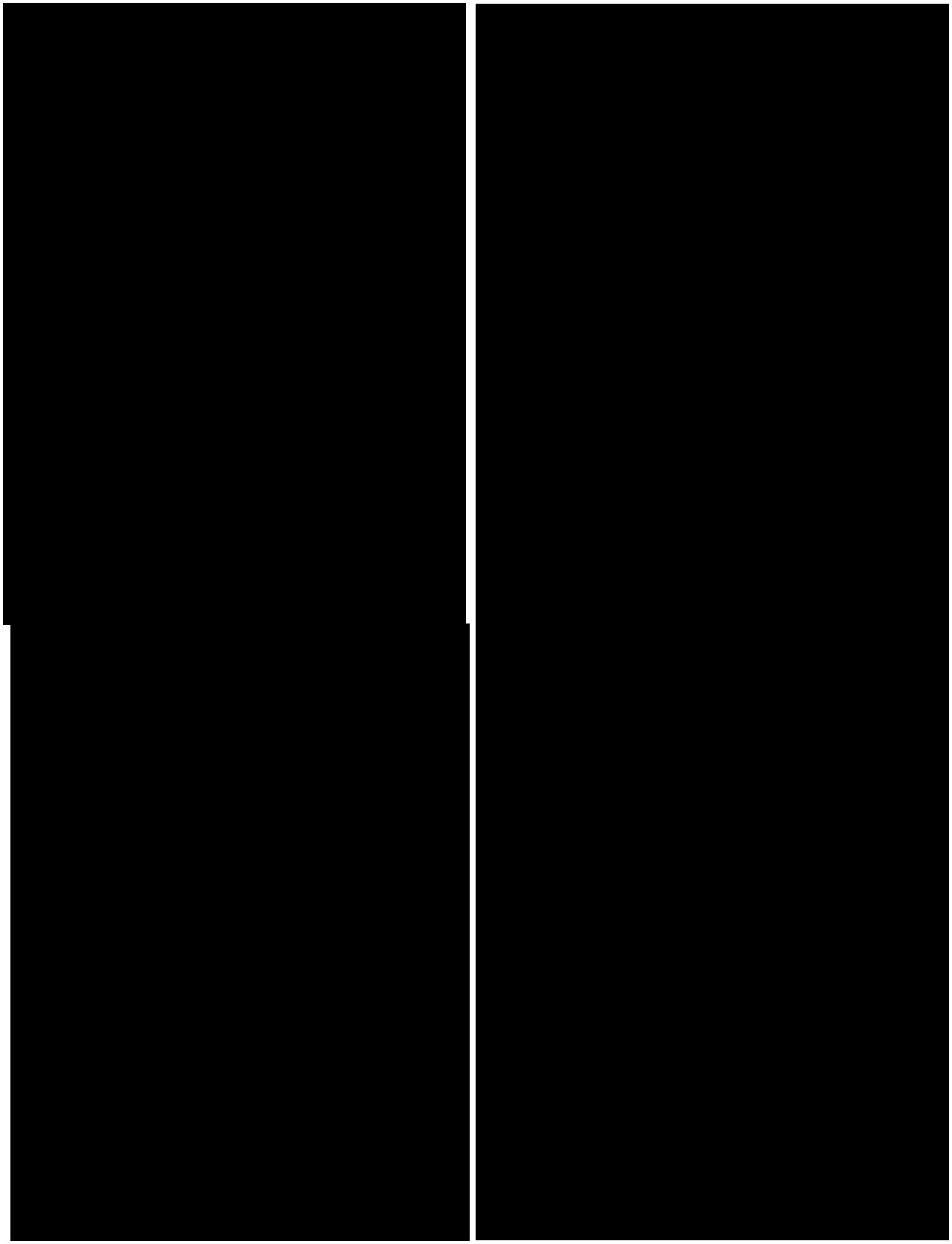
[redacted]

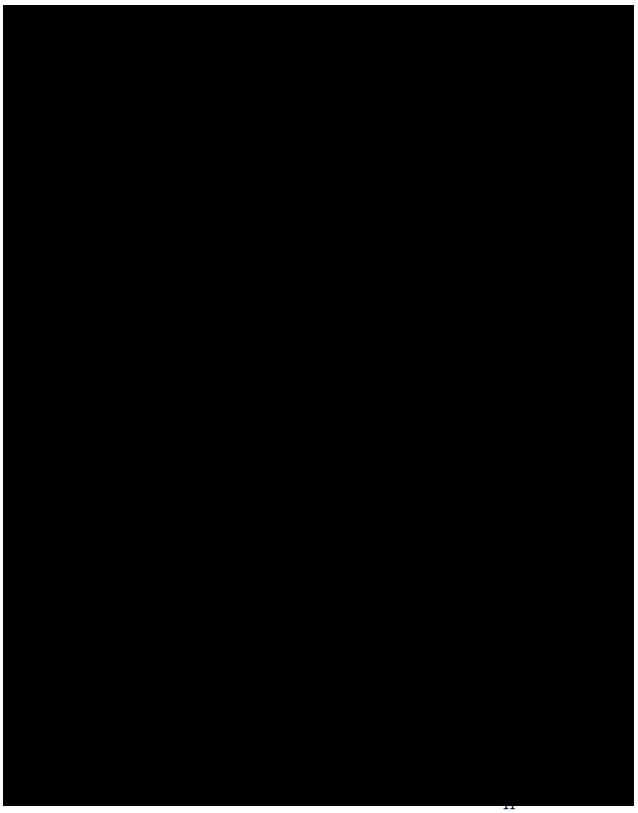
Question 7(a) Business Continuity Plan

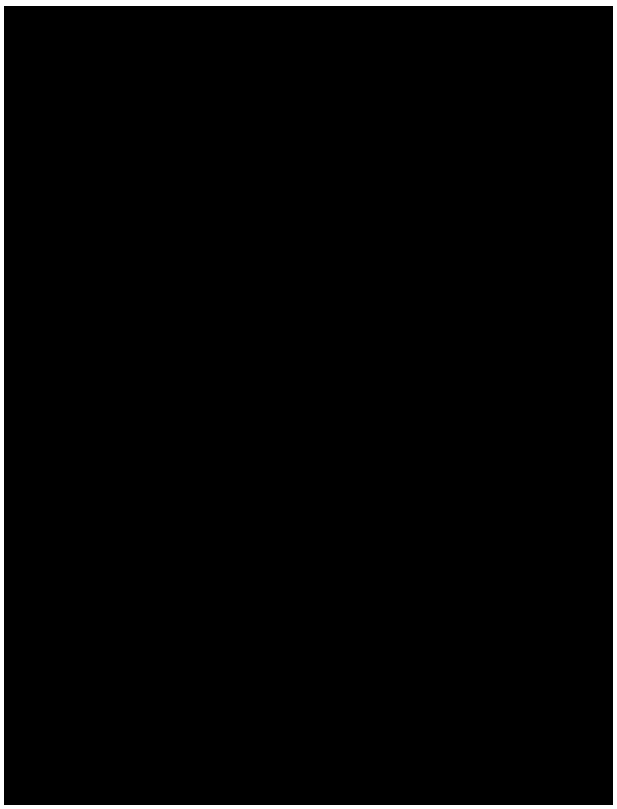





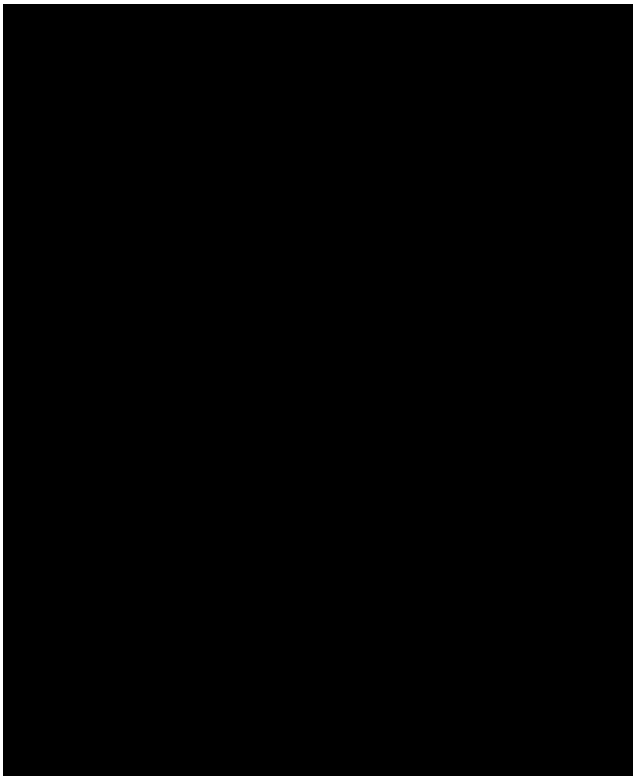


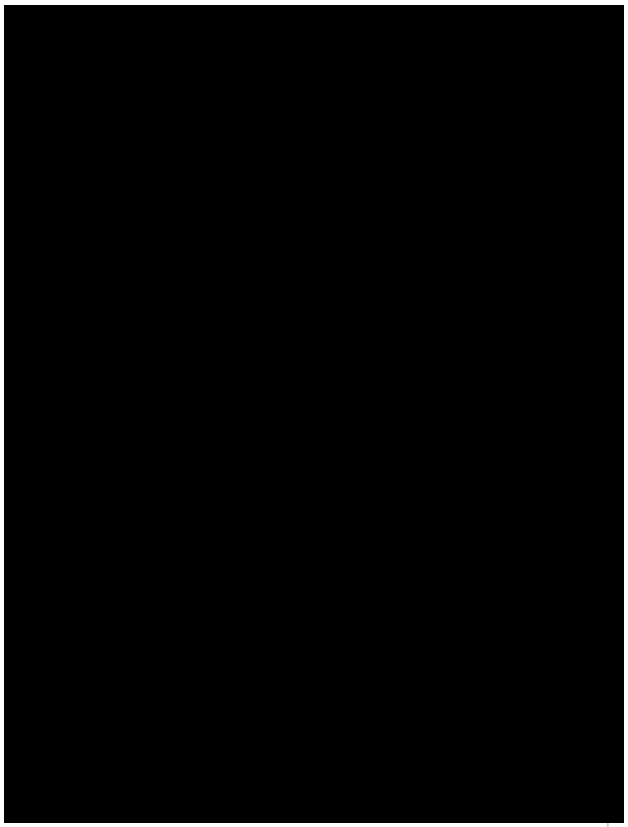
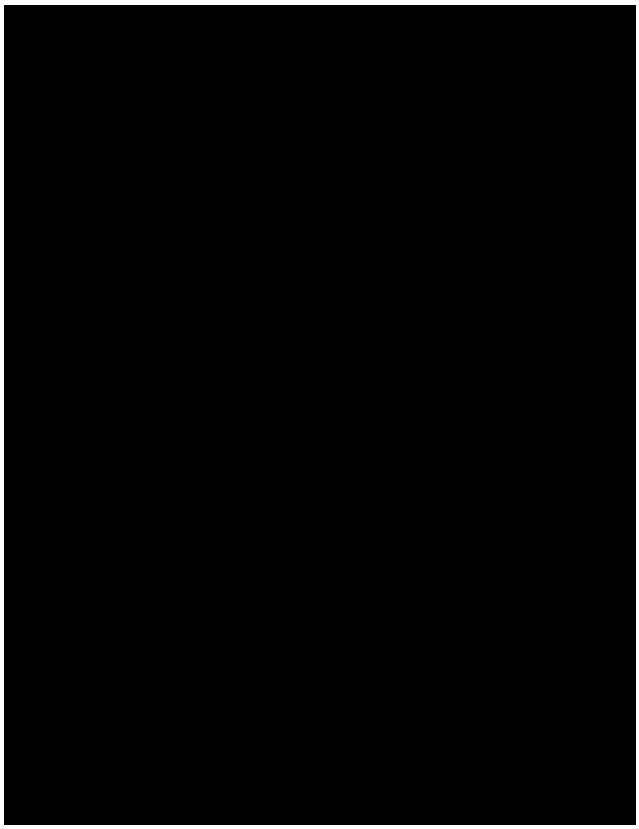


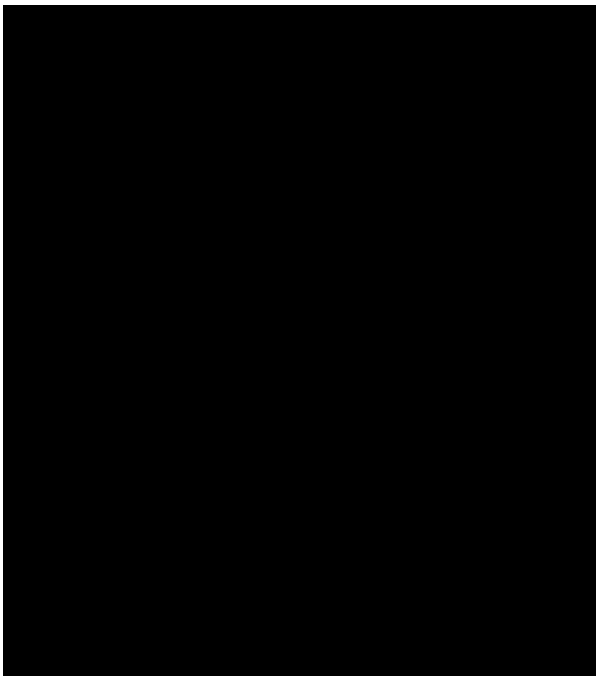


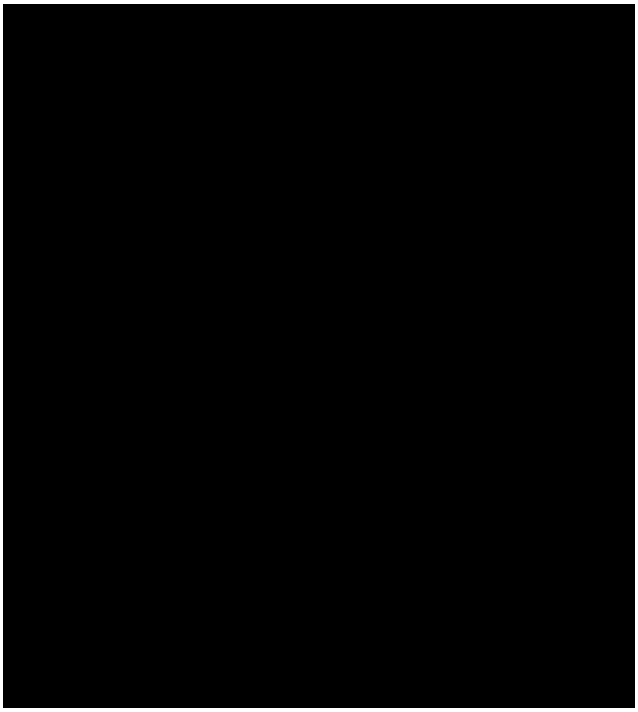


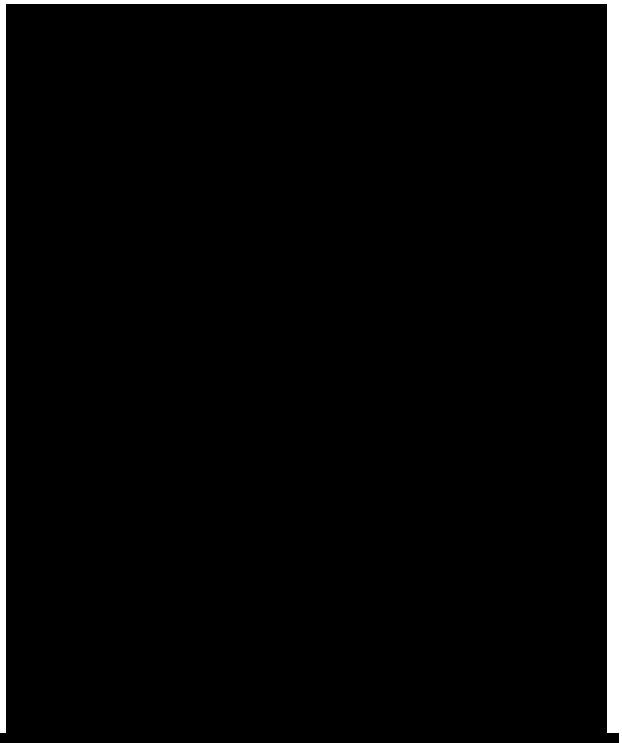


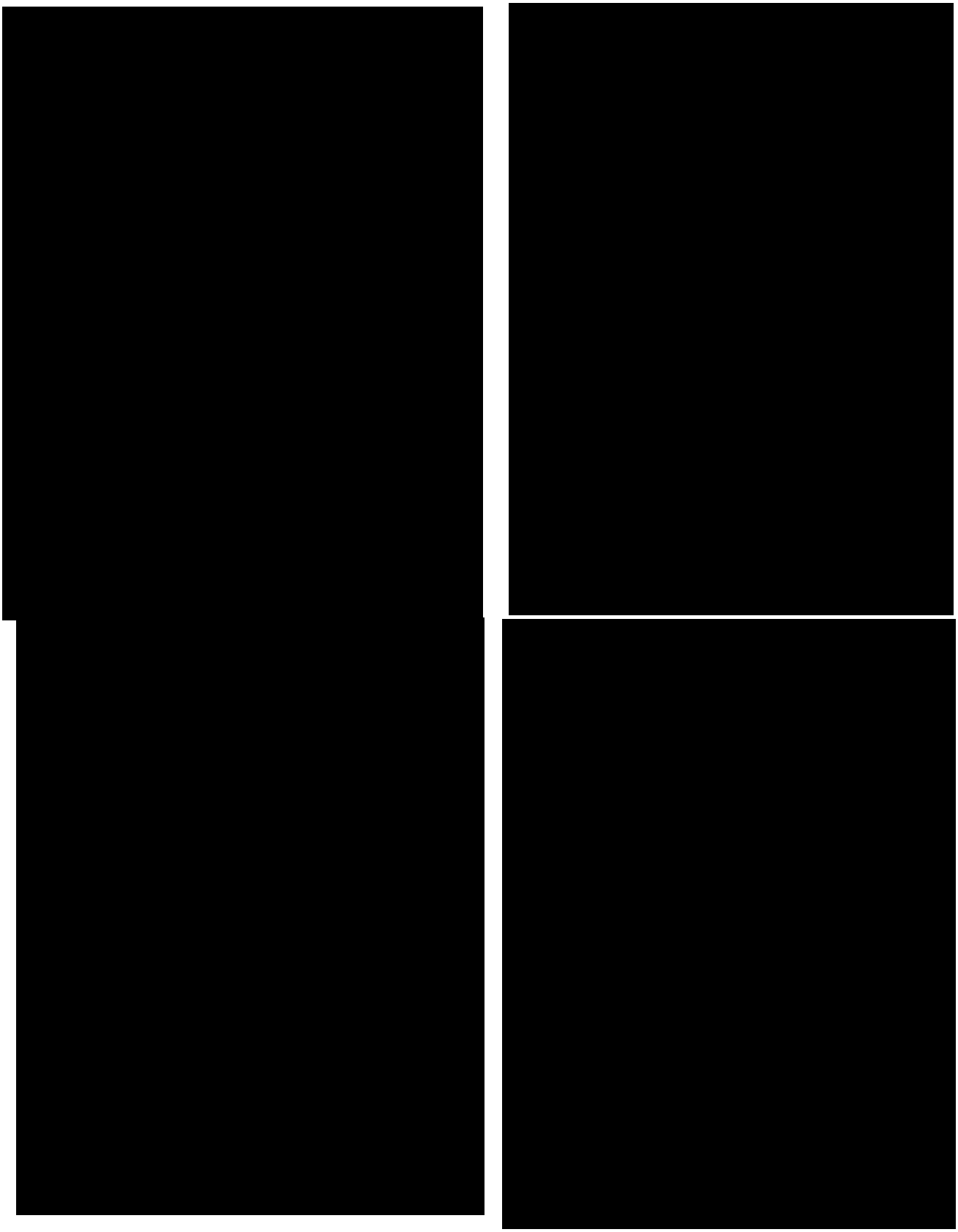


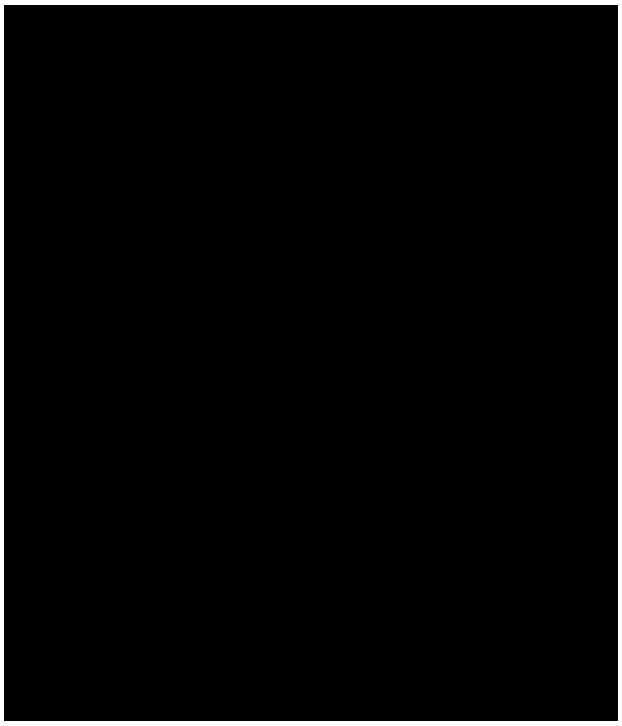
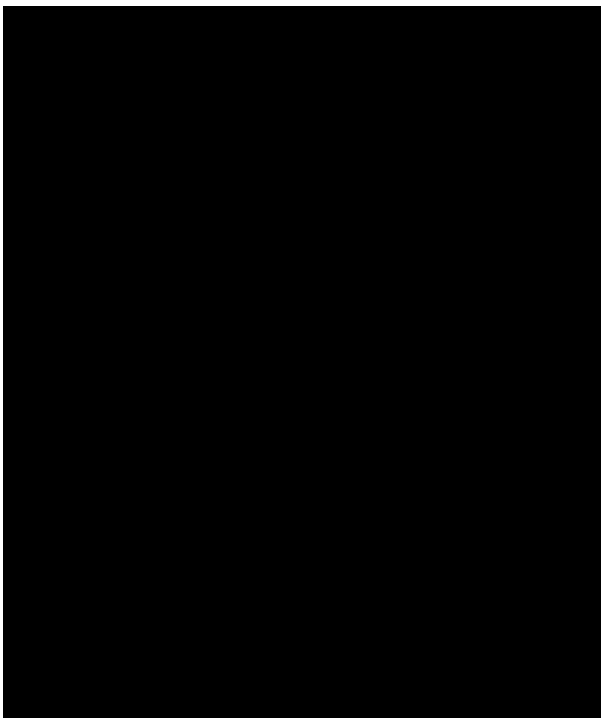
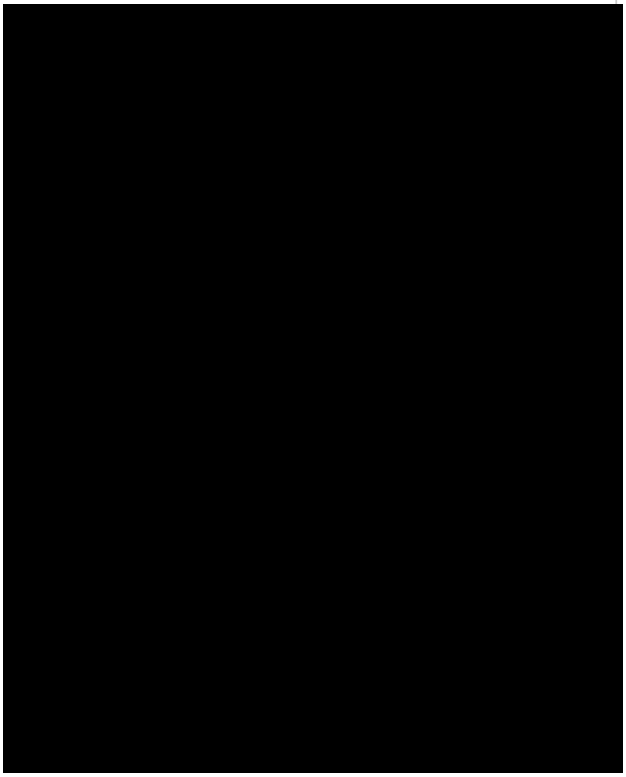
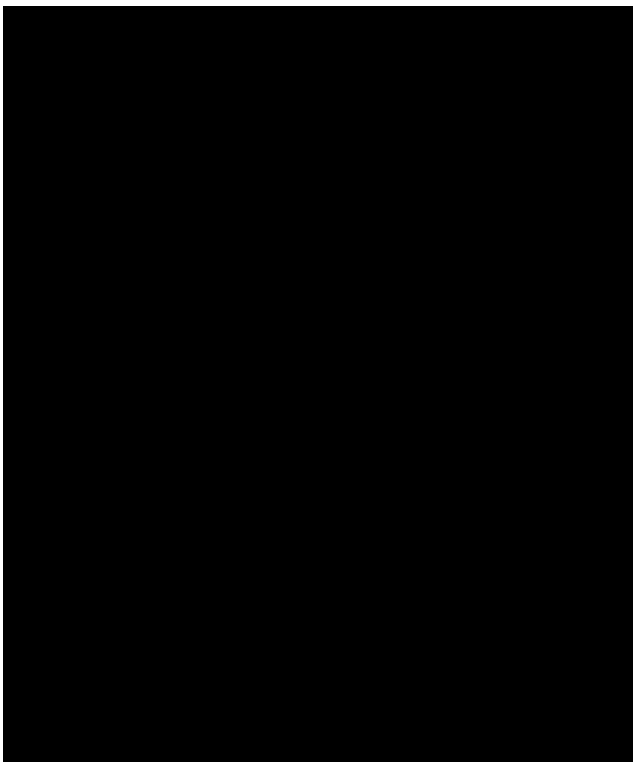



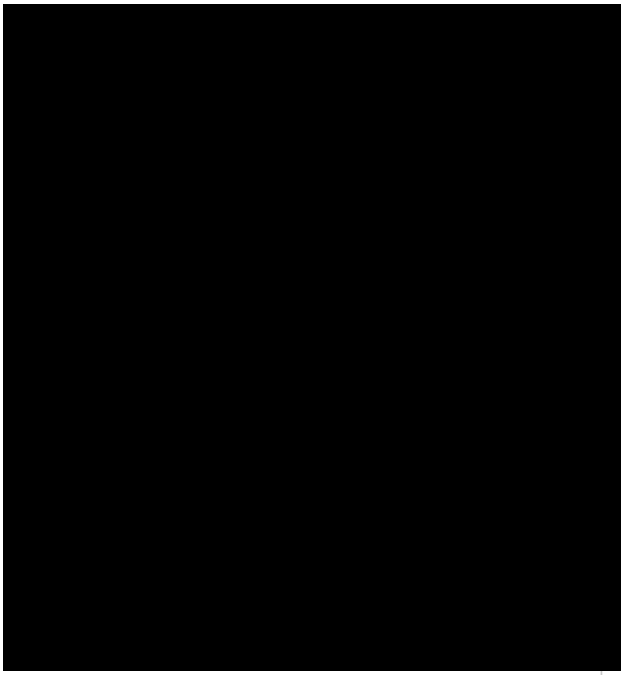
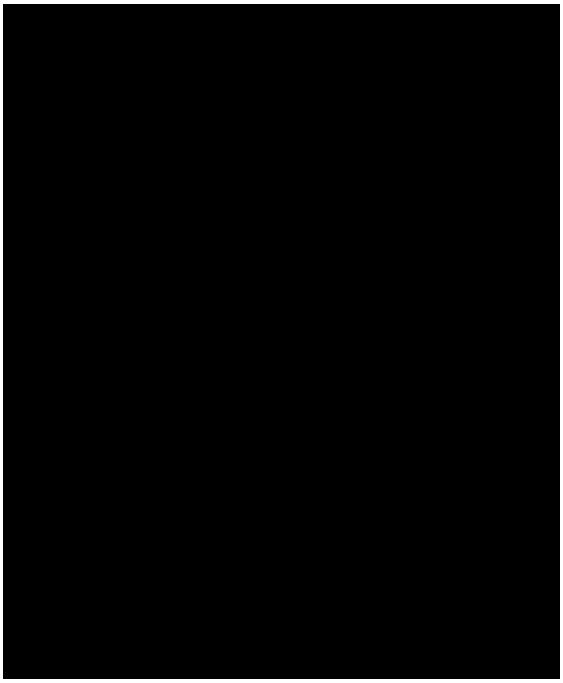
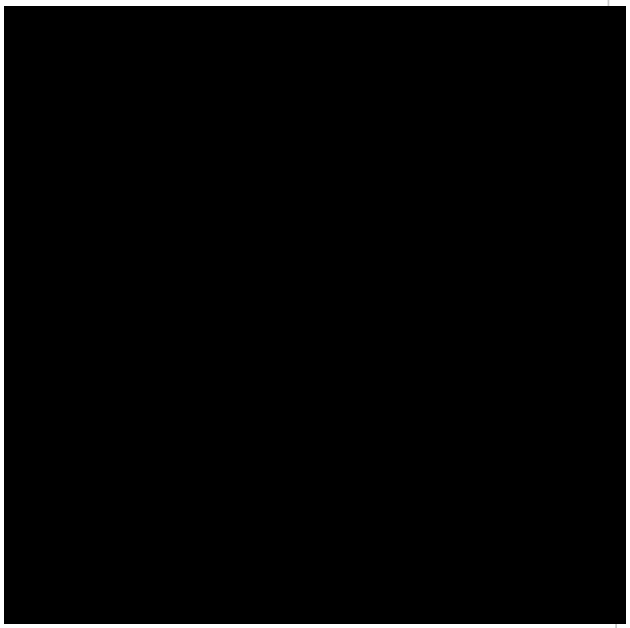
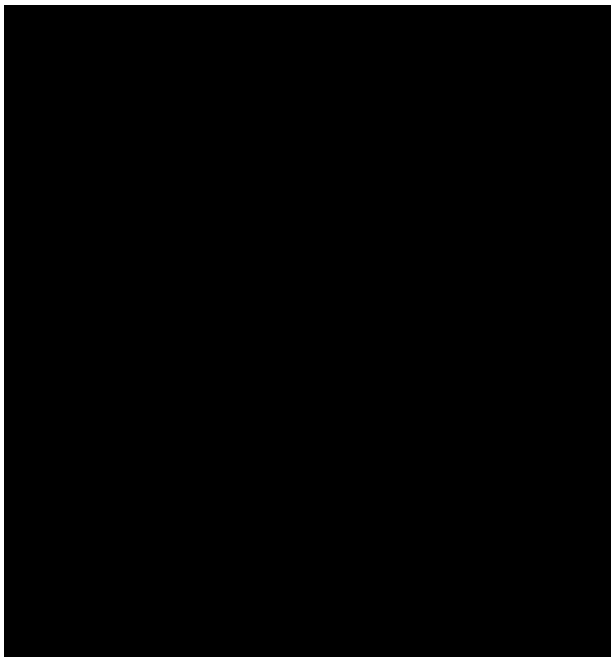






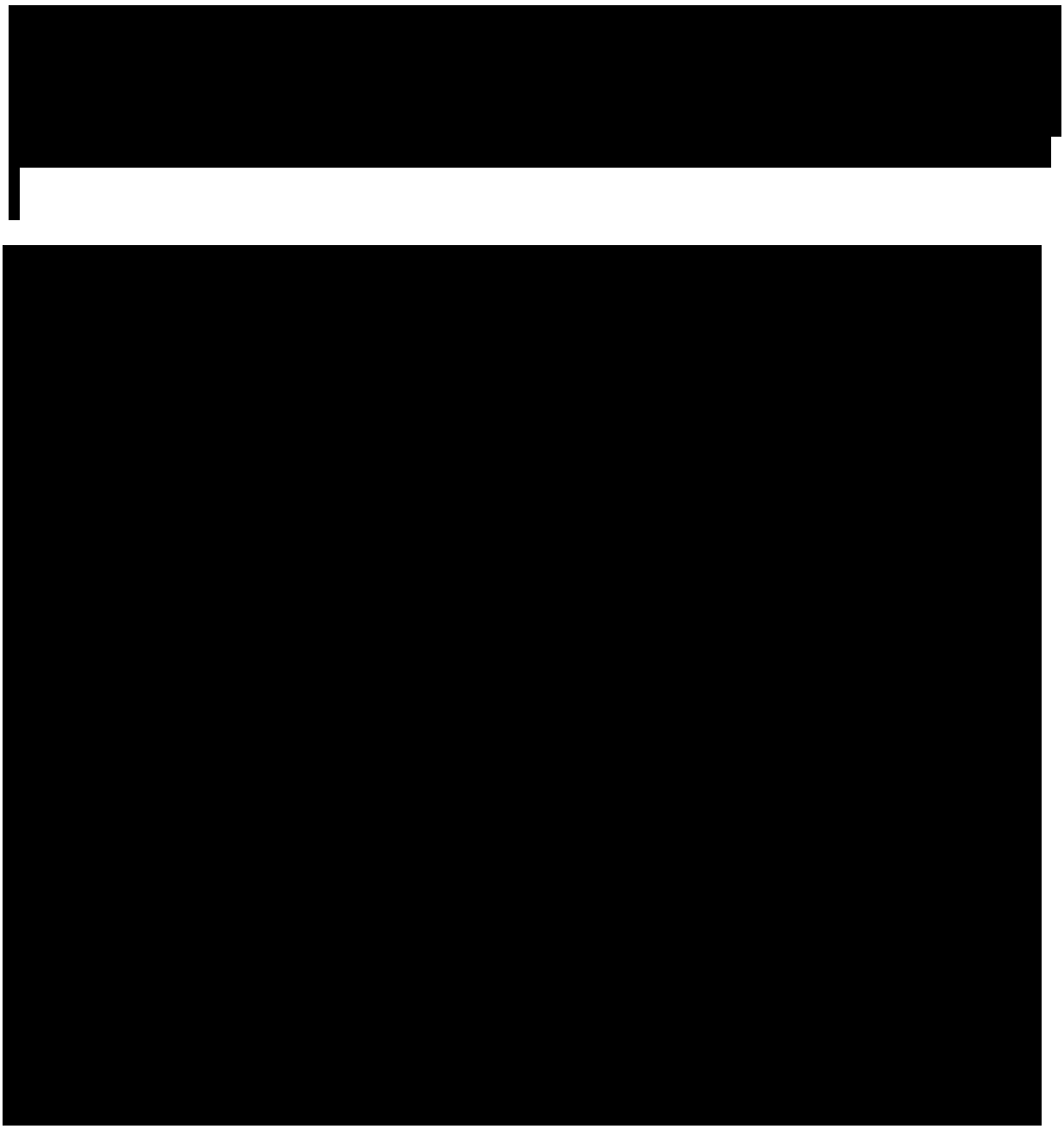


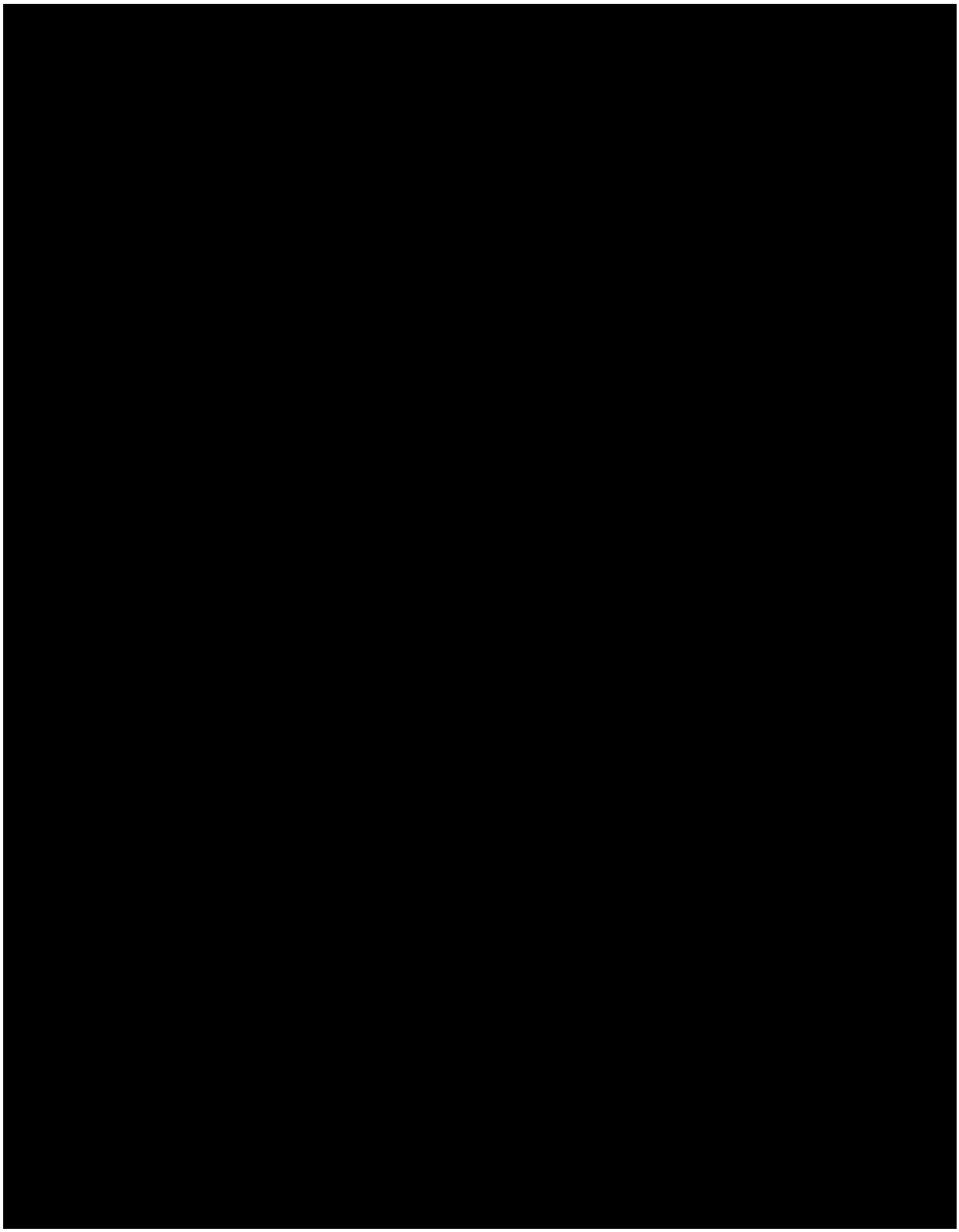





Q7(b) Contingency

Q8 optional Services





SCHEDULE 2 – PAYMENT MECHANISM

1. Monthly Payment

The Monthly Payment shall be the only charge payable by the Authority in respect of the Services and the performance by the Supplier of all other obligations under this Contract.

1.1 Monthly Payment (MP)

(A) The monthly amount payable to the Supplier for the Services (the "**Monthly Payment**") shall be calculated as follows:

MP = FF - FR - ESVC , where:

FF	=	the aggregate Fixed Fees across all Secure Establishments in respect of the relevant Month
FR	=	Financial Remedy relating to Contract Delivery Indicator breach(es) where applied in that Month in accordance with Paragraph 1.5 of this Schedule 2.
ESVC	=	Extended Staffing Vacancy Credit, as calculated in accordance with paragraph 2.6 of this Schedule 2.

(B) The first Monthly Payment shall cover the period from the Services Commencement Date to the end of that Month (pro-rated where the Commencement Date is not the first day of the Month), and the final Monthly Payment shall cover the period from the first day of the final Month of this Contract to the end of the Term (pro-rated where this Contract end date is not the last day of the Month).

1.2 Fixed Fees (FF)

(A) Subject to paragraph 1.2(B) below, the Fixed Fees for each Contract Year shall be set out in the Fees Template and, for additional clarity, the Fixed Fees for each Month in Contract Year 1 shall be as set out in the table in paragraph 5.1 of this Schedule 2

(Payment Mechanism).

(B) The Fixed Fees may be subject to change in accordance with paragraph 3 of this Schedule 2 (Annual Price Review) and paragraph 6 of this Schedule 2 (Change Mechanism) or as otherwise set out in this Contract.

1.3 Contract Delivery Indicators

Where, pursuant to Schedule 10 (Performance Mechanism) a Financial Remedy applies, the Supplier shall apply a credit against the Valid Invoice for the Month following the relevant Performance Quarter or, at the Authority's discretion, any subsequent Month.

1.4 Extended Staffing Vacancies

(A) In the event that a member of Staff who is due to perform an element of the Services becomes unable or unavailable to perform such element of the Services for any reason for a period of time in excess of three (3) Months (an "**Extended Staffing Vacancy**"), the Supplier shall immediately after the expiry of such three (3) Month period notify the Authority with the following information:

(1) details of the member of Staff that is subject to the Extended Staffing Vacancy (the "**Vacant Staff**"), including job role and staffing costs allocated to such Vacant Staff in the Fees Template;

(2) details and evidence of the actions that the Supplier has taken to mitigate the impact of the Extended Staffing Vacancy on the provision of the Services (the "**Mitigation Actions**"); and

(3) the costs incurred by the Supplier in taking the Mitigation Actions, which shall not include business as usual recruitment costs (the "**Mitigation Costs**").

(B) In the event that:

(1) in its reasonable opinion, the Authority considers that Mitigation Actions taken by the Supplier (if any) are inadequate to ensure continuity of the Services in accordance with this Contract; and

(2) as a direct or indirect result of the Extended Staffing Vacancy the Supplier has failed to meet one (1) or more Contract Delivery Indicator(s) in the Month immediately preceding the notification given by the Supplier in accordance with paragraph 1.6(A) above,

the Authority may, for the period that the Extended Staffing Vacancy continues and the Supplier continues to fail to meet one (1) or more Contract Delivery Indicator(s) as a direct or indirect result of the Extended Staffing Vacancy, require the Supplier to issue a credit to the Authority against the subsequent Month's invoice equal to the value of the staffing costs allocated to Vacant Staff in the Fees Template that are not being incurred by the Supplier as a result of the Extended Staffing Vacancy less the reasonable Mitigation Costs incurred by the Supplier in the relevant Month (with the Authority determining what is reasonable for this purpose) (the "**Extended Staffing Vacancy Credit**").

(C) For the avoidance of doubt, if the Mitigation Costs incurred by the Supplier in any Month exceed the staffing costs allocated to Vacant Staff in the Fees Template, the Authority shall not be liable to pay any additional sums to the Supplier.

2. Mobilisation Payment (MobP)

2.1 Mobilisation Payment

(A) The Mobilisation Payment (if applicable) shall cover the Supplier's costs in mobilising and/or transitioning the Services, including, training, recruitment, equipment, mobilisation staff costs and any mobilisation risk pricing included in paragraph 5.2 of this Schedule 2 (Payment Mechanism).

3. Annual Price Review

3.1 The Fixed Fees may be subject to an increase once per Contract Year in accordance with this paragraph 3.

3.2 Any increase agreed by the Authority in accordance with paragraph 3.4 shall be notified to the Supplier in writing, and shall become effective as of 1 April of the upcoming Contract Year (the "**Price Adjustment Date**"). The earliest Price Adjustment Date will be 1 April 2025.

3.3 The Supplier may, on or before 14 March in each Contract Year, submit a written request to the Authority to increase the Fixed Fees in line with indexation, calculated in accordance with paragraph 3.4 below. Any such request shall be accompanied by the Supplier's proposed increase to the Fixed Fees as calculated in accordance with paragraph 3.4, and any other information and documentation that the Authority may request to enable it to determine whether such increase shall be accepted in accordance with the remainder of this paragraph 3.

3.4 The Authority may approve the Supplier's request to increase the Fixed Fees (at its discretion), provided that such increase shall, subject to paragraphs 3.5 to 3.7, in respect of each cost line in the Fees Template, be capped at:

(A) the percentage increase in the:

(i) Average Weekly Earnings Index (AWE-K5DL), in respect of the Fixed Costs in the Fees Template allocated to staffing costs;

(ii) Consumer Prices Index: All Items (CPI-D7BT), in respect of all other Fixed Costs (i.e. non-staffing cost lines), the Management Fee and Operational Risk Payment in the Fees Template,

determined by multiplying the relevant element of the Fixed Fees by the percentage increase in the relevant index (AWE or CPI, as applicable) for the twelve (12) Months ending on the 31 December immediately preceding the relevant Price Adjustment Date (subject to paragraph 3.5 below) (the "**Base Value**"); and

3.5 In the event that:

(A) both the CPI and the AWE indices show a negative percentage value as at 31 December of any Contract Year (as demonstrated in example 3 below); or

(B) either the CPI or AWE index show a negative percentage value as at 31 December of any Contract Year, such that the overall impact on the Fixed Fees would be a negative adjustment,

(a "**Negative Indexation Year**"),

the Supplier shall apply 0% as the sum at Paragraph 3.4(A)(i) or (ii), as

applicable.

3.6 For the avoidance of doubt, where either the CPI or AWE index show a negative percentage value as at 31 December of any Contract Year but the other index shows a positive value, such that the overall impact on the Fixed Fees would be a net positive adjustment (as demonstrated in example 2 below), this shall not constitute a Negative Indexation Year and the CPI and AWE indexation shall be applied to the relevant cost lines (as demonstrated in example 2 below).

3.7 Where in a Contract Year immediately following a Negative Indexation Year the CPI and/or AWE index shows an overall positive percentage value as at 31 December of that Contract Year (i.e. such that that immediately following Contract Year is not a Negative Indexation Year), the Supplier shall use the value as at 31 December in this Contract Year immediately preceding the Negative Indexation Year as the Base Value.

Worked examples:

Example 1 - increase in both indexes

Year	YrX-1	YrX	YrX+1
AWE	500	510	515
AWE rate		2.00%	0.98%
CPI	120	125	130
CPI rate		4.17%	4.00%
Both rates applied to the price			
Staff Costs (AWE)	£ 800	£ 816	£ 824
None Staff Costs (CPI)	£ 200	£ 208	£ 217
Total price	£ 1,000	£ 1,024	£ 1,041

Example 2 - one index increase and one decreases in YrX

Year	YrX-1	YrX	YrX+1
AWE	500	510	515
AWE rate		2.00%	0.98%
CPI	120	115	130
CPI rate		-4.17%	13.04%
Both rates applied to the price as overall still positive			
Staff Costs (AWE)	£ 800	£ 816	£ 824
None Staff Costs (CPI)	£ 200	£ 192	£ 217
Total price	£ 1,000	£ 1,008	£ 1,041

Example 3 - decrease in both indexes in YrX

Year	YrX-1	YrX	YrX+1
AWE	500	495	515
AWE rate		-1.00%	4.04%
AWE rate - applied as		0.00%	3.00%
CPI	120	115	130
CPI rate		-4.17%	13.04%
CPI rate - applied as		0.00%	8.33%
Combined rate is negative so in YrX no change and in YrX+1 compared to Yr-1			
Staff Costs (AWE)	£ 800	£ 800	£ 824
None Staff Costs (CPI)	£ 200	£ 200	£ 217
Total price	£ 1,000	£ 1,000	£ 1,041

In all examples the YrX+1 price gives the same price (for the same index), even though the YrX price differs.

3.8 Following receipt of notice that a price increase has been accepted in accordance with paragraph 3.4 (if applicable), the Supplier shall prepare an updated Fees Template to apply in respect of the upcoming Contract Year (i.e. applicable between 1 April and 31 March the following year), to reflect the approved increase to the Fixed Fees. Such updated Fees Template shall also take into account any amendments required as a result of any changes implemented in accordance with paragraph 6 of this Schedule 2 (Change Mechanism).

4. Invoicing and Payment

4.1 The Supplier shall submit an accurate Valid Invoice for the Monthly Payment calculated in accordance with paragraph 1 of this Schedule 2 to the Authority no later than ten (10) Business Days after the end of the Month of actual service provision.

4.2 Invoices may not be dated any earlier than the last day of the Month of actual Service provision and the date the Authority receives the invoice, or the invoice's actual date, shall be the binding date that determines payment, whichever is the later.

4.3 The Authority shall pay each Valid Invoice in accordance with Clause C1.18 of this Contract.

5. Fees

5.1 Fixed Fees (FF)

The Fixed Fees for each Contract Year shall be set out in the Fees Template (subject to change in accordance with paragraph 1.2(B) of this Schedule 2) and, for additional clarity, the Fixed Fees for the first Contract Year shall be as set out below:

Annual Fixed Fees for Contract Year 1 *(Aggregate of all Fixed Fees in Contract Year 1)*	[redacted]
Monthly Fixed Fees for Contract Year 1 *(Aggregate of all Fixed Fees for Contract Year 1 divided by 9, being the number of Months in Contract Year 1)*	The payments for Year 1 are made up of a first payment of [redacted] and then 8 payments of [redacted]

5.2 Mobilisation Payment (MobP)

(A) There is no Mobilisation Payment due to the Supplier under this Contract. For the avoidance of any doubt, the Supplier shall have no entitlement to receive any costs or payment in connection with the mobilisation of the services pursuant to this Contract.

(B) Not used.

6. Change Mechanism

6.1 Establishment Service Cessation Deduction

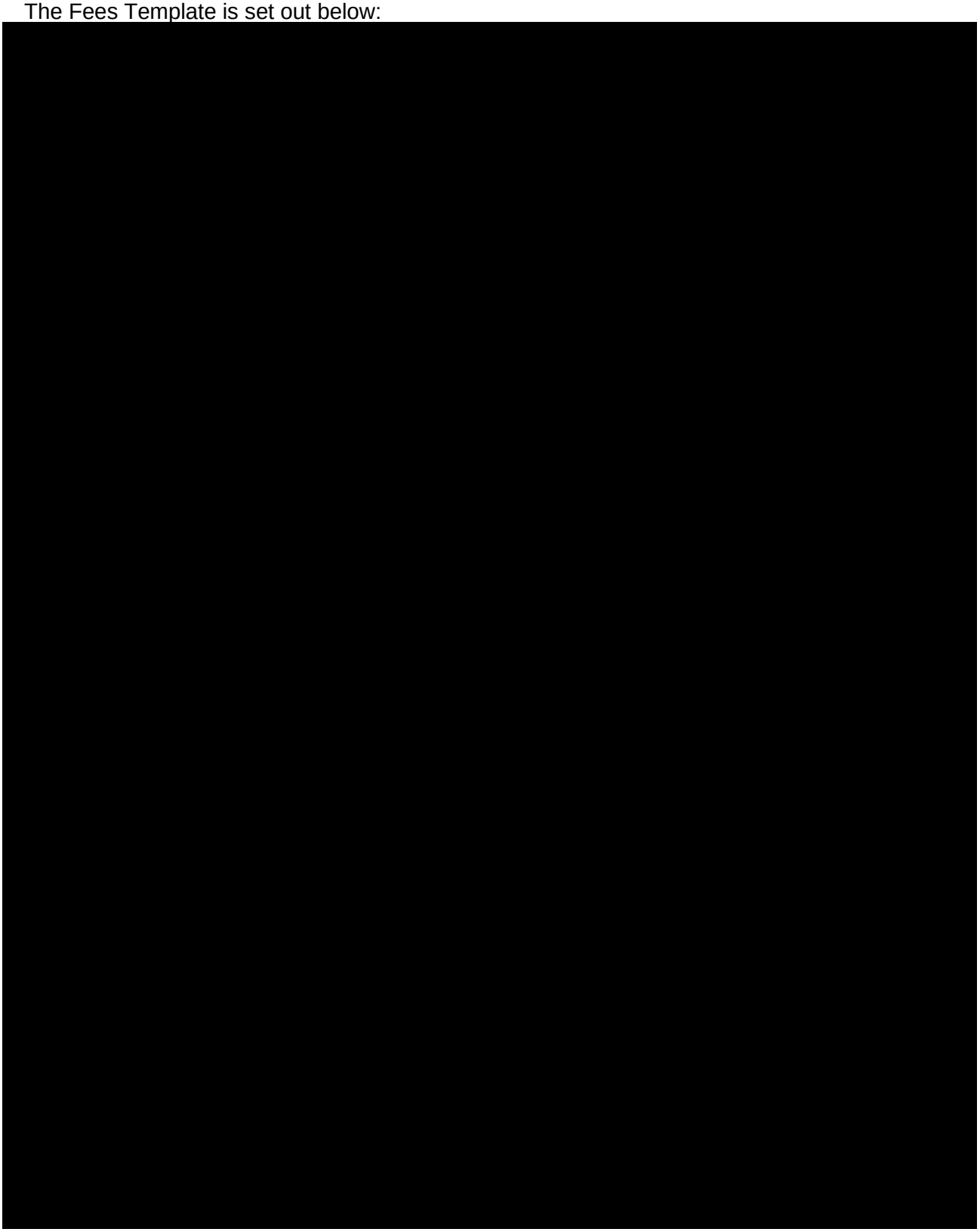
The Fixed Fees may be subject to change in accordance with clause C4 (Establishment Service Cessation Deduction).

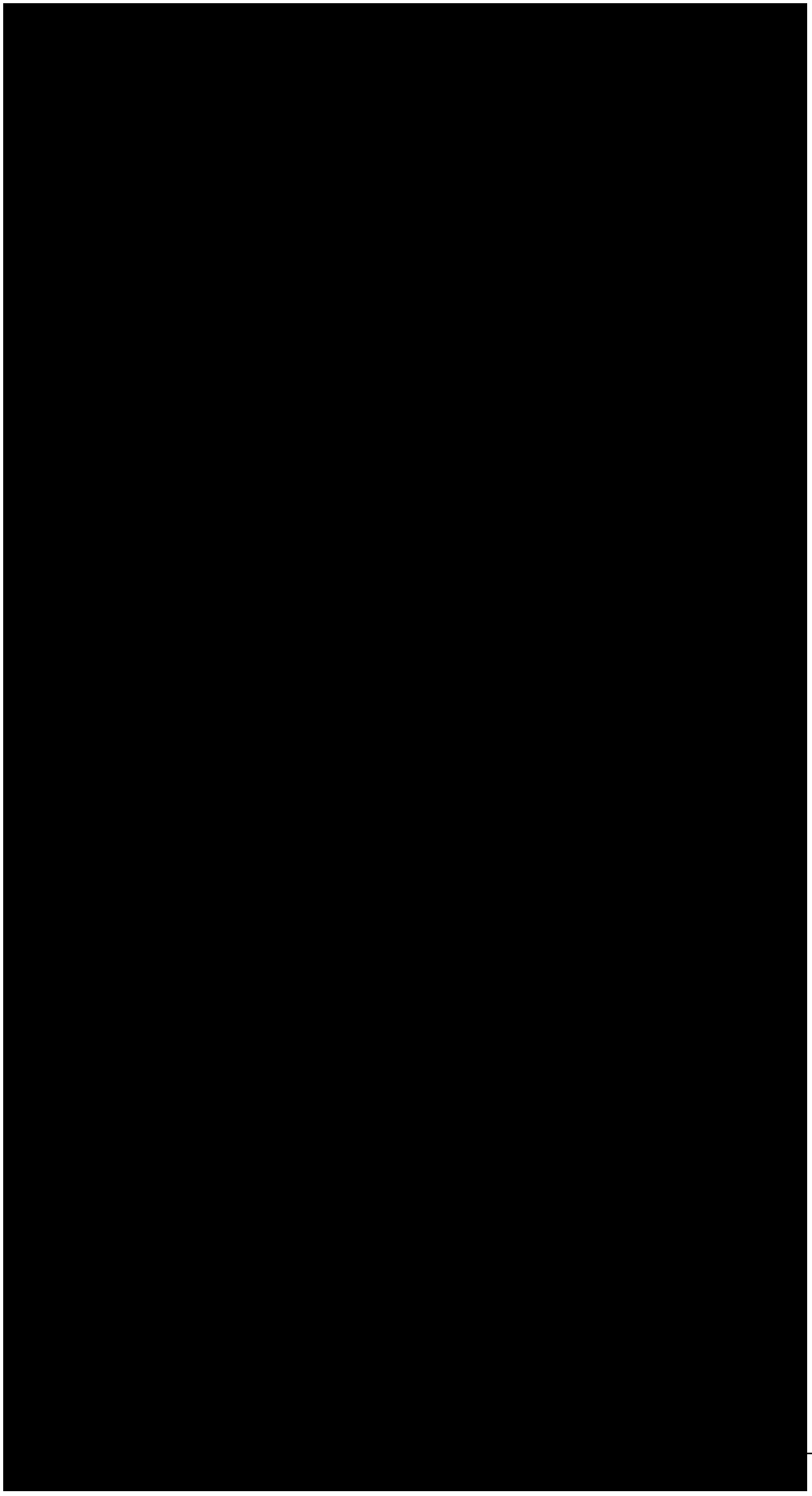
6.2 Addition of new Secure Establishments

Where the Authority requires Services to be provided in respect of a new secure establishment in accordance with paragraph 3 of Schedule 7 (Secure Establishments), the Supplier shall submit to the Authority such pricing information as the Authority may request, including any amendment to the Fixed Fees that would be required in order for the Supplier to provide the Services in respect of such new Secure Establishment. Such pricing shall be proportionate to the Fixed Fees included in Appendix A of this Schedule 2 (Fees Template) and the principles set out therein, having regard to the Authority's particular requirements in relation to the new Secure Establishment.

ANNEX A: Fees Template

The Fees Template is set out below:





77781672.1877781672.18

83423154.1

77781672.1877781672.18

83423154.1

SCHEDULE 3 - CHANGE CONTROL

Change Request Form

(For completion by the Party requesting the Change)

Contract Title:	**Party requesting Change:**
Name of Supplier:	
Change Request Number:	**Proposed Change implementation date:**
Full description of requested Change (including proposed changes to wording of the Contract where possible):	
Reasons for requested Change:	
Effect of requested Change	
Assumptions, dependencies, risks and mitigation (if any):	
Change Request Form prepared by (name):	
Signature:	
Date of Change Request:	

Contract Change Notice ("CCN")

(For completion by the Authority once the Change has been agreed in principle by both Parties. Changes do not become effective until this form has been signed by both Parties.)

Contract Title:	**Change requested by:**
Name of Supplier:	
Change Number:	
Date on which Change takes effect:	
Contract between: The [Secretary of State for Justice]/[The Lord Chancellor] [delete as applicable] and [insert name of Supplier]	
It is agreed that the Contract is amended, in accordance with Regulation 72 of the Public Contracts Regulations 2015, as follows: [Insert details of the variation (including any change to the Price and deliverables/obligations) based on the information provided in the Change Request Form and any subsequent discussions/negotiations, cross referencing the wording of the original Contract, as previously changed (if applicable), where possible] **Where significant changes have been made to the Contract, information previously published on Contracts Finder will be updated.**	
Words and expressions in this CCN shall have the meanings given to them in this Contract. The Contract, including any previous CCNs, shall remain effective and unaltered except as amended by this CCN	

Signed for and on behalf of [the Secretary of State for Justice]/[the Lord Chancellor]		**Signed for and on behalf of [insert name of Supplier]**	
Signature		**Signature**	
Name		**Name**	
Title		**Title**	
Date		**Date**	

SCHEDULE 4 - COMMERCIALLY SENSITIVE INFORMATION

1 Without prejudice to the Authority's general obligation of confidentiality, the Parties acknowledge that the Authority may have to disclose Information in or relating to this Contract following a Request for Information pursuant to clause D5 (Freedom of Information).

2 In this Schedule 4 the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be contrary to the public interest.

3 Where possible the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule 4 applies.

4 Without prejudice to the Authority's obligation to disclose Information in accordance with the FOIA and the EIR, the Authority will, acting reasonably but in its sole discretion, seek to apply the commercial interests exemption set out in s.43 of the FOIA to the Information listed below.

SUPPLIER'S COMMERCIALLY SENSITIVE INFORMATION	DATE	DURATION OF CONFIDENTIALITY
Supplier's Proposals set out at Annex A of Schedule 1	N/A	Duration of the Contract
Fees Template set out at Annex A of Schedule 2	N/A	Duration of the Contract
Draft business continuity plan set out at Annex A Schedule 11	N/A	Duration of the Contract
Outline Mobilisation Plan set out at Annex 1 of Schedule 13	N/A	Duration of the Contract

SCHEDULE 5 - SUPPLIER AND THIRD PARTY SOFTWARE

Supplier Software comprises the following:
Supplier Software comprises the following:

Software	Supplier (if Affiliate of the Supplier)	Purpose	No. of Licences	Restrictions	No. of copies	Other	To be deposited in escrow?
NONE	**NONE**	**NONE**	**NONE**	**NONE**	**NONE**	**NONE**	**NONE**

Third Party Software comprises the following:

Third Party Software	Supplier	Purpose	No. of Licences	Restrictions	No. of copies	Other	To be deposited in escrow?
Office 365 Apps for Enterprise	**Microsoft**	**Collaboration suite**	**1 licence per user**	**None**	**1 copy per PC**	**Users also have access to the Web version**	**N/A**
Enterprise Connect	**OpenText**	**Service User recording**	**1 licence per user**	**None**	**1 copy per PC**		**N/A**
Chrome	**Google**	**Internet browser**	**N/A (free software)**	**None**	**1 copy per PC**		**N/A**
Client Connector	**Zscaler**	**Secures access to the Internet and hosted applications**	**1 licence per user**	**None**	**1 copy per PC**		**N/A**
Dragon NaturallySpeaking	**Nuance**	**Speech recognition**	**1 licence per user as recommended by Access to Work**	**None**	**1 copy per PC**		**N/A**
PowerBI	**Microsoft**	**Access to PowerBI dashboards**	**1 licence per user**	**None**	**N/A (Web App)**		**N/A**

Acrobat Reader	**Adobe**	**For viewing PDF files**	**N/A (free software)**	**None**	**1 copy per PC**		**N/A**

SCHEDULE 6 – INFORMATION SECURITY AND ASSURANCE

1.1 This Schedule 6 sets out:

(a) the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Contract to ensure the security of the Authority Data and the Information Management System;

(b) the Certification Requirements applicable to the Supplier and each of those Sub-contractors which Processes Authority Data;

(c) the security requirements in annex 1, with which the Supplier must comply;

(d) the tests which the Supplier shall conduct on the Information Management System during the Term; and

(e) the Supplier's obligations to:

(i) return or destroy Authority Data on the expiry or earlier termination of this Contract; and

(ii) prevent the introduction of Malicious Software into the Supplier System and to scan for, contain the spread of, and minimise the impact of Malicious Software which is introduced into the Supplier System in paragraph 9; and

(iii) report Breaches of Security to the Authority.

2 Principles of Security

2.1 The Supplier acknowledges that the Authority places great emphasis on the confidentiality, integrity and availability of the Authority Data and, consequently on the security of:

(a) the Premises;

(b) the ICT Environment;

(c) the Information Management System; and

(d) the Services.

2.2 Notwithstanding the involvement of the Authority in assessing the arrangements which the Supplier implements to ensure the security of the Authority Data and the Information Management System, the Supplier is and remains responsible for:

(a) the security, confidentiality, integrity and availability of the Authority Data whilst that Authority Data is under the control of the Supplier or any of its Sub-Contractors; and

(b) the security of the Information Management System.

2.3 The Supplier shall:

(a) comply with the security requirements in annex 1; and

(b) ensure that each Sub-Contractor that Processes Authority Data complies with the Sub-Contractor Security Requirements.

2.4 The Supplier shall provide the Authority with access to Staff responsible for information assurance to facilitate the Authority's assessment of the Supplier's compliance with its obligations set out in this Schedule 6 at reasonable times on reasonable notice.

3 Information Security Approval Statement

3.1 The Supplier shall ensure that its Mobilisation Plan sets out in sufficient detail how it will ensure compliance with the requirements of this Schedule 6, including any requirements imposed on Sub-Contractors by annex 2, from the Commencement Date.

3.2 The Supplier may not use the Information Management System to Process Authority Data unless and until:

(a) the Supplier has procured the conduct of an IT Health Check of the Supplier System by a CHECK Service Provider in accordance with paragraph 7.1; and

(b) the Authority has issued the Supplier with an Information Security Approval Statement in accordance with the process set out in this paragraph 3.

3.3 The Supplier shall document in the Security Management Plan how the Supplier and its Sub-Contractors shall comply with the requirements set out in this Schedule and this Contract in order to ensure the security of the Authority Data and the Information Management System.

3.4 The Supplier shall prepare and submit to the Authority within 20 Working Days of the Commencement Date, the Security Management Plan, which comprises:

(a) an Information Assurance Assessment;

(b) the Required Changes Register; and

(c) the Incident Management Process.

3.5 The Authority shall review the Supplier's proposed Security Management Plan as soon as possible and, in any event within 20 Working Days of receipt and shall either issue the Supplier with:

(a) an Information Security Approval Statement, which shall confirm that the Supplier may use the Information Management System to Process Authority Data; or

(b) a rejection notice, which shall set out the Authority's reasons for rejecting the Security Management Plan.

3.6 If the Authority rejects the Supplier's proposed Security Management Plan, the Supplier shall take the Authority's reasons into account in the preparation of a revised Security Management Plan, which the Supplier shall submit to the Authority for review within 10 Working Days or such other timescale as agreed with the Authority.

3.7 The Authority may require, and the Supplier shall provide the Authority and its authorised representatives with:

(a) access to the Staff;

(b) access to the Information Management System to audit the Supplier and its Sub-contractors' compliance with this Contract; and

(c) such other information and/or documentation that the Authority or its authorised representatives may reasonably require,

to assist the Authority to establish whether the arrangements which the Supplier and its Sub-Contractors have implemented in order to ensure the security of the Authority Data and the Information Management System are consistent with the representations in the Security Management Plan. The Supplier shall provide the access required by the Authority in accordance with this paragraph 3 within 10 Working Days of receipt of such request, except in the case of a Breach of Security in which case the Supplier shall provide the Authority with the access that it requires within 24 hours of receipt of such request.

4 Compliance Reviews

4.1 The Supplier shall regularly review and update the Security Management Plan, and provide such to the Authority, at least once each year and as required by this paragraph 4.

4.2 The Supplier shall undertake scanning with the minimum frequencies according with the MOJ Vulnerability Scanning Policy, Vulnerability Scanning Guide – Security Guidance (justice.gov.uk), and notify the Authority within 2 Working Days of identifying:

(a) a significant change to the components or architecture of the Information Management System;

(b) a new risk to the components or architecture of the Information Management System;

(c) a vulnerability to the components or architecture of the Service which is classified 'Medium', 'High', 'Critical' or 'Important' in accordance with the classification methodology set out in paragraph 9.2 to this Schedule 6;

(d) a change in the threat profile;

(e) a significant change to any risk component;

(f) a significant change in the quantity of Personal Data held within the Service;

(g) a proposal to change any of the Premises; and/or

(h) an ISO/IEC 27001 (at least ISO/IEC 27001:2022) audit report produced in connection with the Certification Requirements indicates significant concerns.

4.3 Within 10 Working Days of notifying the Authority or such other timescale as may be agreed with the Authority, the Supplier shall make the necessary changes to the Required Changes Register including implementing patches in line with the extant MOJ Patch management policy (Patch Management Guide – Security Guidance (justice.gov.uk)) and submit the updated Required Changes Register the Authority for review and approval.

4.4 Where the Supplier is required to implement a change, including any change to the Information Management System, the Supplier shall effect such change at its own cost.

5 Certification Requirements

5.1 The Supplier shall be certified compliant with:

(a) the prevailing version of ISO/IEC 27001 by a UK Accreditation Service-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001 (new certifications assessed to ISO 27001 2022; an existing at least ISO/IEC 27001:2013); and

(b) Cyber Essentials PLUS

and shall provide the Authority with a copy of each such certificate of compliance before the Supplier is permitted to receive, store or Process Authority Data.

5.2 The Supplier shall ensure that each Higher Risk Sub-contractor is certified compliant with either:

(a) the prevailing version of ISO/IEC 27001 by a UK Accreditation Service (UKAS)-approved certification body or is included within the scope of an existing certification of compliance with ISO/IEC 27001 (at least ISO/IEC 27001:2013); or

(b) Cyber Essentials PLUS

and must provide the Authority with a copy of each such certificate of compliance before the Higher-Risk Sub-contractor is permitted to receive, store or Process Authority Data.

5.3 The Supplier shall ensure that each Medium Risk Sub-contractor is certified compliant with Cyber Essentials.

5.4 The Supplier shall ensure that the Supplier and each Sub-Contractor who is responsible for the secure destruction of Authority Data:

(a) securely destroys Authority Data only at Premises which are included within the scope of an existing certification of compliance with the prevailing published ISO/IEC 27001;

(b) satisfies the Authority that their data destruction/deletion practices comply with UK GDPR and follows all relevant NCSC guidance; and

(c) maintains an asset register of all Authority supplied information, data and equipment to ensure Authority assets are returned and/or deleted.

5.5 The Supplier shall provide the Authority with evidence of its and Sub-Contractors' compliance with the requirements set out in this paragraph 6 before the Supplier or the relevant Sub-Contractor (as applicable) may carry out the secure destruction of any Authority Data.

5.6 The Supplier shall notify the Authority as soon as reasonably practicable and, in any event within 2 Working Days, if the Supplier or any Sub-Contractor ceases to be compliant with the Certification Requirements and, on request from the Authority, shall or shall procure that the relevant Sub-Contractor shall:

(a) immediately cease using the Authority Data; and

(b) procure that the relevant Sub-Contractor promptly returns, destroys and/or erases the Authority Data in accordance with the requirements set out in this paragraph 5.

5.7 The Authority may exempt, in whole or part, the Supplier or any Sub-Contractor from the requirements of this paragraph 5. Any exemption must be in writing to be effective. The Supplier shall include the exemption in the Security Management Plan.

6 Security Testing

6.1 The Supplier shall, at its own cost procure and conduct:

(a) testing of the Information Management System by a CHECK Service Provider ("**IT Health Check**"); and

(b) such other security tests as may be required by the Authority.

6.2 The Supplier shall:

(a) complete all of the above security tests before:

(i) the Supplier submits the Security Management Plan to the Authority for review in accordance with paragraph 3; and

(ii) before the Supplier is given permission by the Authority to Process or manage any Authority Data

(b) repeat the IT Health Check not less than once every 12 Months during the Term and submit the results of each such test to the Authority for review in accordance with this paragraph 6.

6.3 In relation to each IT Health Check, the Supplier shall:

(a) agree with the Authority the aim and scope of the IT Health Check;

(b) promptly, and no later than 10 Working Days, following the receipt of each IT Health Check report, provide the Authority with a copy of the full report;

(c) if the IT Health Check report identifies any vulnerabilities, the Supplier shall, in line with the MOJ Patch management policy (Patch Management Guide – Security Guidance (justice.gov.uk)):

(i) prepare a remedial plan for approval by the Authority (each a "**Remediation Plan**") which sets out in respect of each vulnerability identified in the IT Health Check report:

(A) how the vulnerability will be remedied;

(B) unless otherwise agreed in writing between the Parties, the date by which the vulnerability will be remedied, which must be:

(1) within 3 Months of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of "medium";

(2) within 7 Calendar Days of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of "high"; and

(3) within 7 Calendar Days of the date the Supplier received the IT Health Check report in the case of any vulnerability categorised with a severity of “critical”;

(C) the tests which the Supplier shall perform or procure to be performed (which may, at the discretion of the Authority, include a further IT Health Check) to confirm that the vulnerability has been remedied;

(ii) comply with the Remediation Plan; and

(iii) conduct such further tests on the Service as are required by the Remediation Plan to confirm that the Remediation Plan has been complied with.

6.4 The Supplier shall ensure that any testing which could adversely affect the Supplier System shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such tests shall be agreed in advance with the Authority.

6.5 If any testing conducted by or on behalf of the Supplier identifies a new risk, new threat, vulnerability or exploitation technique that has the potential to affect the security of the Information Management System, the Supplier shall, within 2 Working Days of becoming aware of such risk, threat, vulnerability or exploitation technique, provide the Authority with a copy of the test report and:

(a) propose interim mitigation measures to vulnerabilities in the Information Management System known to be exploitable where a security patch is not immediately available; and

(b) where and to the extent applicable, remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the Supplier System) within the timescales set out in the test report or such other timescales as may be agreed with the Authority.

6.6 The Supplier shall conduct such further tests of the Supplier System as may be required by the Authority from time to time to demonstrate compliance with its obligations set out this Schedule 6 and this Contract.

6.7 The Supplier shall notify the Authority immediately if it fails to, or believes that it will not, mitigate the vulnerability within the timescales set out in paragraph 6.3.

7 Security Monitoring and Reporting

7.1 The Supplier shall:

(a) monitor the delivery of assurance activities;

(b) maintain and update the Security Management Plan in accordance with paragraph 4;

(c) agree a document which presents the residual security risks to inform the Authority's decision to Approve the Supplier to Process and transit the Authority Data;

(d) monitor security risk impacting upon the operation of the Service;

(e) report Breaches of Security in accordance with the approved Incident Management Process; and

(f) agree with the Authority the frequency and nature of the security reports to be prepared and submitted by the Supplier to the Authority within 20 Working Days of the Commencement Date.

8 Malicious Software

8.1 The Supplier shall install and maintain Anti-Malicious Software or procure that Anti-Malicious Software is installed and maintained on any part of the Information Management System which may Process Authority Data and ensure that such Anti-Malicious Software is configured to perform automatic software and definition updates as well as regular scans of the Information Management System to check for, prevent the introduction of Malicious Software or where Malicious Software has been introduced into the Information Management System, to identify, contain the spread of, and minimise the impact of Malicious Software.

8.2 If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Authority Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

8.3 Any cost arising out of the actions of the Parties taken in compliance with paragraph 8.2 shall be borne by the Parties as follows:

(a) by the Supplier where the Malicious Software originates from:

(i) the Supplier Software;

(ii) the Third Party Software supplied by the Supplier; or

(iii) the Authority Data whilst the Authority Data is or was under the control of the Supplier

(i) unless, in the case of the Authority Data only, the Supplier can demonstrate that such Malicious Software was present in the Authority Data and not quarantined or otherwise identified by the Authority when the Authority provided the Authority Data to the Supplier; and

(b) by the Authority, in any other circumstance.

9 Breach of Security

9.1 If either Party becomes aware of a Breach of Security it must notify the other in accordance with the Incident Management Process.

9.2 The Incident Management Process must, as a minimum, require the Supplier to do the following when it becomes aware of a Breach of Security or attempted Breach of Security:

(a) immediately take all reasonable steps necessary to:

(i) minimise the extent of actual or potential harm caused by such Breach of Security;

(ii) remedy such Breach of Security to the extent possible;

(iii) apply a tested mitigation against any such Breach of Security; and

(iv) prevent a further Breach of Security in the future which exploits the same root cause failure;

(b) as soon as reasonably practicable and, in any event, within 1 hour of identification, following the Breach of Security or attempted Breach of Security, provide to the Authority full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Authority. The Supplier should additionally report the Breach of Security to the HMPPS Information & Security incident reporting line by calling telephone number (0203) 334 0324.

9.3 If any action is taken in response to a Breach of Security or attempted Breach of Security as a result of non-compliance by the Supplier, its Sub-contractors and/or all or any part of the Information Management System with this Contract, then such remedial action must be completed at no additional cost to the Authority.

ANNEX 1: SECURITY REQUIREMENTS

1 Security Classification of Information

1.1 If the provision of the Services requires the Supplier to Process Authority Data which is classified as:

(a) OFFICIAL-SENSITIVE, the Supplier shall implement procedures at no less than the that mandated by Government Security Classification guidelines (Government Security Classifications Policy (HTML) - GOV.UK (www.gov.uk)), as well as any such additional measures as agreed with the Authority from time to time in order to ensure that such information is safeguarded in accordance with the applicable Standards.

2 End User Devices

2.1 The Supplier shall manage, and shall ensure that all Sub-Contractors manage, all end-user devices used by the Supplier on which Authority Data is Processed in accordance the following requirements:

(a) the operating system and any applications that Process or have access to Authority Data must be in current support by the vendor, or the relevant community in the case of Open Source operating systems or applications;

(b) users must authenticate before gaining access;

(c) all Authority Data is encrypted using an encryption tool agreed by the Authority;

(d) the end-user device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the end-user device is inactive;

(e) the end-user device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Authority Data;

(f) the Suppler or Sub-Contractor, as applicable, can, without physical access to the end-user device, remove or make inaccessible all Authority Data on the device and prevent any user or group of users from accessing the device;

(g) all end-user devices are within in the scope of any current Cyber Essentials Plus certificate held by the Supplier, or any prevailing ISO/IEC 27001 certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.

2.2 The Supplier shall comply, and ensure that all Sub-Contractors comply, with the recommendations in NCSC Device Guidance and prevailing Authority Technical Security Guidance, as updated, amended or replaced from time to time, as if those recommendations were incorporated as specific obligations under this Contract.

2.3 Where there any conflict between the requirements of this Schedule 6and the requirements of the NCSC Device Guidance and/or the Authority's Technical Security Guidance, the requirements of this Schedule 6 takes precedence.

3 Encryption

3.1 The Supplier shall ensure, and shall ensure that all Sub-contractors ensure, that Authority Data is encrypted:

(a) when stored at any time when no operation is being performed on it; and

(b) when transmitted.

3.2 Where the Supplier, or a Sub-Contractor, cannot encrypt Authority Data the Supplier shall:

(a) immediately inform the Authority of the subset or subsets of Authority Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;

(b) provide details of the protective measures the Supplier or Sub-Contractor (as applicable) proposes to take to provide equivalent protection to the Authority as encryption; and

(c) provide the Authority with such information relating to the Authority Data concerned, the reasons why that Authority Data cannot be encrypted and the proposed protective measures as the Authority may require.

3.3 The Authority, the Supplier and, where the Authority requires, any relevant Sub-Contractor shall meet to agree appropriate protective measures for the unencrypted Authority Data.

3.4 Where the Authority and Supplier reach agreement, the Supplier must update the Security Management Plan to include:

(a) the subset or subsets of Authority Data not encrypted and the circumstances in which that will occur; and

(b) the protective measure that the Supplier and/or Sub-contractor will put in please in respect of the unencrypted Authority Data.

3.5 Where the Authority and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Authority that it could not encrypt certain Authority Data, either Party may refer the matter to be determined in accordance with the dispute resolution procedure set out in clause I1.

4 Personnel Security

4.1 All Staff are subject to a pre-employment check before they may participate in the provision and or management of the Services which must include all pre-employment checks which are required by the BPSS including: verification of the individual's identity; verification of the individual's nationality and immigration status; verification of the individual's employment history; and verification of the individual's criminal record. The pre-employment checks in relation to any Staff who are not directly employed by the Supplier must include a BPSS Enhanced Check Level 1.

4.2 The Parties shall review the roles and responsibilities of the Staff who will be involved in the management and/or provision of the Services in order to enable the Authority to determine which roles require additional vetting and a specific national security vetting clearance (for example a Counter Terrorist Check). Roles which are likely to require additional vetting and a specific national security vetting clearance include system administrators whose role would provide those individuals with privileged access to systems which Process Authority Data or data which, if it were Authority Data, would be classified as OFFICIAL-SENSITIVE.

4.3 The Supplier shall not allow Staff who fail the security checks required by paragraphs 4.1 and 4.2 to be involved in the management and/or provision of the Services except where the Authority has expressly agreed in writing to the involvement of the named individual in the management and/or provision of the Services. The Supplier shall provide an up to date list of all Staff and their associated security clearance checks each month, including all Sub-contractor personnel and the personnel of any sub-contractor of a Sub-contractor who in each case are involved in the management and/or provision of the Services.

4.4 The Supplier shall ensure that Staff are granted such access to Authority Data only as is necessary to enable the Staff to perform their role and to fulfil their responsibilities.

4.5 The Supplier shall ensure that Staff who no longer require access to the Authority Data (for example. they cease to be employed by the Supplier or any of its Sub-contractors), have their rights to access the Authority Data revoked within one Working Day.

4.6 The Supplier shall ensure that Staff who have access to the Premises, the ICT Environment or the Authority Data receive regular training on security awareness that reflects the degree of access those individuals have to the Premises, the ICT Environment or the Authority Data.

4.7 The Supplier shall ensure that the training provided to Staff under paragraph 4.6 includes training on the identification and reporting fraudulent communications intended to induce individuals to disclose Personal Data or any other information that

could be used, including in combination with other Personal Data or information, or with other techniques, to facilitate unauthorised access to the Premises, the ICT Environment or the Authority Data ("phishing").

5 Identity, Authentication and Access Control

5.1 The Supplier shall operate an access control regime to ensure:

(a) all users and administrators of the Supplier System are uniquely identified and authenticated when accessing or administering the Services; and

(b) all persons who access the Premises are identified and authenticated before they are allowed access to the Premises.

5.2 The Supplier shall apply the 'principle of least privilege' when allowing persons access to the Supplier System and Premises so that such persons are allowed access only to those parts of the Premises and the Supplier System they require.

5.3 The Supplier shall retain records of access to the Premises and to the Supplier System and shall make such record available to the Authority on request.

6 Data Destruction or Deletion

6.1 The Supplier shall:

(a) prior to securely sanitising any Authority Data or when requested the Supplier shall provide the Authority with all Authority Data in an agreed open format;

(b) have documented processes to ensure the availability of Authority Data if the Supplier ceases trading;

(c) securely erase in a manner agreed with the Authority any or all Authority Data held by the Supplier when requested to do so by the Authority;

(d) securely destroy in a manner agreed with the Authority all media that has held Authority Data at the end of life of that media in accordance with any specific requirements in this Contract and, in the absence of any such requirements, as agreed by the Authority; and

(e) implement processes which address the NCSC guidance on secure sanitisation.

7 Audit and Protective Monitoring

7.1 The Supplier shall collect audit records which relate to security events in the Information Management System or that would support the analysis of potential and actual

compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include regular reports and alerts setting out details of access by users of the Information Management System, to enable the identification of (without limitation) changing access trends, any unusual patterns of usage and/or accounts accessing higher than average amounts of Authority Data.

7.2 The Parties shall work together to establish any additional audit and monitoring requirements for the Information Management System.

7.3 The Supplier shall discuss with the Authority the retention periods for audit records and event logs which, when agreed with the Authority, shall be documented in the Security Management Plan.

8 Location of Authority Data

8.1 The Supplier shall not and shall procure that none of its Sub-Contractors Process Authority Data outside the UK without Approval.

9 Vulnerabilities and Corrective Action

9.1 The Parties acknowledge that from time to time vulnerabilities in the Information Management System may be discovered which, unless mitigated, will present an unacceptable risk to the Authority Data.

9.2 The severity of vulnerabilities for COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the Security Management Plan and using the appropriate vulnerability scoring systems including:

(a) the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST at http://nvd.nist.gov/cvss.cfm); and

(b) Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

9.3 Subject to paragraph 9.4, the Supplier shall procure the application of security patches to vulnerabilities in the Information Management System within:

(a) 7 days after the public release of patches for those vulnerabilities categorised as 'Critical';

(b) 30 days after the public release of patches for those vulnerabilities categorised as 'Important'; and

(c) 30 days after the public release of patches for those vulnerabilities categorised as 'Other'.

9.4 The timescales for applying patches to vulnerabilities in the Information Management System set out in paragraph 9.3 shall be extended where:

(a) the Supplier can demonstrate that a vulnerability in the Information Management System is not exploitable within the context of the Services (for example, because it resides in a Software component which is not involved in running in the Services) provided such vulnerabilities shall be remedied by the Supplier within the timescales set out in paragraph 9.3 if the vulnerability becomes exploitable within the context of the Services;

(b) the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Authority; or

(c) the Authority agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the Security Management Plan.

9.5 The Security Management Plan shall include provisions for major version upgrades of all COTS Software to be kept up to date such that all COTS Software are always in mainstream support throughout the Term unless otherwise agreed by the Authority in writing. All COTS Software should be no more than N-1 versions behind the latest software release.

10 Secure Architecture

10.1 The Supplier shall design the Information Management System in accordance with:

(a) the NCSC "Security Design Principles for Digital Services", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/security-design-principles-digital-services-main;

(b) the NCSC "Bulk Data Principles", a copy of which can be found at https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main; and

(c) the NSCS "Cloud Security Principles", a copy of which can be found at: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles and which are summarised below:

(i) "Cloud Security Principle 1: data in transit protection" which, amongst other matters, requires that user data transiting networks should be adequately protected against tampering and eavesdropping;

(ii) "Cloud Security Principle 2: asset protection and resilience" which, amongst other matters, requires that user data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure;

(iii) "Cloud Security Principle 3: separation between users" which, amongst other matters, requires that a malicious or compromised user of the service should not be able to affect the service or data of another;

(iv) "Cloud Security Principle 4: governance framework" which, amongst other matters, requires that the Supplier should have a security governance framework which coordinates and directs its management of the Services and information within it;

(v) "Cloud Security Principle 5: operational security" which, amongst other matters, requires that the Services need to be operated and managed securely in order to impede, detect or prevent a Breach of Security;

(vi) "Cloud Security Principle 6: personnel security" which, amongst other matters, requires that where Supplier Personnel have access to Authority Data and/or the Authority System that those personnel be subject to appropriate security screening and regular security training;

(vii) "Cloud Security Principle 7: secure development" which, amongst other matters, requires that the Services be designed and developed to identify and mitigate threats to their security;

(viii) "Cloud Security Principle 8: supply chain security" which, amongst other matters, requires the Supplier to ensure that appropriate security controls are in place with its Sub-contractors and other suppliers;

(ix) "Cloud Security Principle 9: secure user management" which, amongst other matters, requires the Supplier to make the tools available for the Authority to securely manage the Authority's use of the Service;

(x) "Cloud Security Principle 10: identity and authentication" which, amongst other matters, requires the Supplier to implement appropriate controls in order to ensure that access to Service interfaces is constrained to authenticated and authorised individuals;

(xi) "Cloud Security Principle 11: external interface protection" which, amongst other matters, requires that all external or less trusted

interfaces with the Services should be identified and appropriately defended;

(xii) "Cloud Security Principle 12: secure service administration" which, amongst other matters, requires that any ICT system which is used for administration of a cloud service will have highly privileged access to that service;

(xiii) "Cloud Security Principle 13: audit information for users" which, amongst other matters, requires the Supplier to be able to provide the Authority with the audit records it needs to monitor access to the Service and the Authority Data held by the Supplier and/or its Sub-contractors; and

(xiv) "Cloud Security Principle 14: secure use of the service" which, amongst other matters, requires the Supplier to educate Supplier Personnel on the safe and secure use of the Information Management System.

(d) the Authority's Technical Security Guidance

ANNEX 2: SECURITY REQUIREMENTS FOR SUB-CONTRACTORS

1 Application of Annex

1.1 This annex 2 applies to all Sub-Contractors which Process Authority Data.

1.2 The Supplier shall:

(a) ensure that those Sub-Contractors comply with the provisions of this annex 2; and

(b) keep sufficient records to demonstrate that compliance to the Authority.

2 Designing and managing secure solutions

2.1 The Sub-Contractor shall implement its solution to mitigate the security risks in accordance with the NCSC's Cyber Security Design Principles https://www.ncsc.gov.uk/collection/cyber-security-design-principles.

2.2 The Sub-Contractor shall assess its systems against the NCSC Cloud Security Principles:

https://www.ncsc.gov.uk/collection/cloud-security?curPage=/collection/cloud-security/implementing-the-cloud-security-principles

at its own cost to demonstrate that the people, process, technical and physical controls have been delivered in an effective way. The Sub-Contractor shall document that assessment and make that documentation available to the Authority on the Authority's request.

3 Data Processing, Storage, Management and Destruction

3.1 The Sub-Contractor shall not Process any Authority Data outside the UK. The Authority may allow the Sub-Contractor to Process Authority Data outside the UK and may impose conditions on that permission, with which the Sub-Contractor shall comply. Any permission must be in writing to be effective.

3.2 The Sub-Contractor shall, when requested to do so by the Authority:

(a) securely destroy Authority Data only on Premises which are included within the scope of an existing certification of compliance with ISO/IEC 27001 or later (at least ISO/IEC 27001:2013);

(b) satisfy the Authority that its data destruction/deletion practices comply with UK GDPR requirements and follows all relevant NCSC guidance; and

(c) maintain an asset register of all Authority supplied information, data and equipment to ensure Authority assets are returned and/or deleted.

4 Personnel Security

4.1 The Sub-Contractor shall perform appropriate checks on their staff before they may participate in the provision and or management of the Services. Those checks must include all pre-employment checks required by the BPSS including: verification of the individual's identity; verification of the individual's nationality and immigration status; verification of the individual's employment history; and verification of the individual's criminal record.

4.2 The Sub-Contractor shall, if the Authority requires, at any time, ensure that one or more of the Sub-Contractor's staff obtains Security Check clearance in order to Process Authority Data containing Personal Data above certain volumes specified by the Authority, or containing Special Category Personal Data.

4.3 Any Sub-Contractor staff who will, when performing the Services, have access to a person under the age of 18 years must undergo Disclosure and Barring Service checks.

5 End User Devices

5.1 The Supplier shall manage, and shall ensure that all Sub-contractors manage, all end-user devices used by the Supplier on which Authority Data is Processed in accordance with the following requirements:

(a) the operating system and any applications that Process or have access to Authority Data must be in current support by the vendor, or the relevant community in the case of Open Source operating systems or applications;

(b) users must authenticate before gaining access;

(c) all Authority Data must be encrypted using an encryption tool agreed to by the Authority;

(d) the end-user device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the end-user device is inactive;

(e) the end-user device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Authority Data;

(f) the Suppler or Sub-contractor, as applicable, can, without physical access to the end-user device, remove or make inaccessible all Authority Data on

the device and prevent any user or group of users from accessing the device;

(g) all end-user devices are within in the scope of any current Cyber Essentials Plus certificate held by the Supplier, or any ISO/IEC 27001 or later (at least ISO/IEC 27001:2022) certification issued by a UKAS-approved certification body, where the scope of that certification includes the Services.

5.2 The Supplier shall comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance and Authority Technical Security Guidance, as updated, amended or replaced from time to time, as if those recommendations were incorporated as specific obligations under this Contract.

5.3 Where there any conflict between the requirements of this Schedule 6 and the requirements of the NCSC Device Guidance, the requirements of this Schedule 6 takes precedence.

6 Encryption

6.1 The Supplier shall ensure, and shall ensure that all Sub-contractors ensure, that Authority Data is encrypted:

(a) when stored at any time when no operation is being performed on it; and

(b) when transmitted.

6.2 Where the Supplier or a Sub-Contractor cannot encrypt Authority Data the Supplier shall:

(a) immediately inform the Authority of the subset or subsets of Authority Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;

(b) provide details of the protective measures the Supplier or Sub-Contractor (as applicable) proposes to take to provide equivalent protection to the Authority as encryption; and

(c) provide the Authority with such information relating to the Authority Data concerned, the reasons why that Authority Data cannot be encrypted and the proposed protective measures as the Authority may require.

6.3 The Authority, the Supplier and, where the Authority requires, any relevant Sub-Contractor shall meet to agree appropriate protective measures for the unencrypted Authority Data.

6.4 Where the Authority and Supplier reach agreement, the Supplier shall update the Security Management Plan to include:

(a) the subset or subsets of Authority Data not encrypted and the circumstances in which that will occur; and

(b) the protective measure that the Supplier and/or Sub-Contractor will put in please in respect of the unencrypted Authority Data.

6.5 Where the Authority and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Authority that it could not encrypt certain Authority Data, either Party may refer the matter to be determined in accordance with the dispute resolution procedure set out in clause I1.

7 Patching and Vulnerability Scanning

7.1 The Sub-Contractor shall proactively monitor supplier vulnerability websites and ensure all necessary patches and upgrades are applied to maintain security, integrity and availability in accordance with the NCSC Cloud Security Principles.

8 Third Party Sub-contractors

8.1 The Sub-Contractor shall not transmit or disseminate the Authority Data to any other person unless Approved.

8.2 The Sub-Contractor shall not, when performing any part of the Services, use any software to Process the Authority Data where the licence of that software purports to grant the licensor rights to Process the Authority Data greater than those rights strictly necessary for the use of the software.

ANNEX 3: SECURITY MANAGEMENT PLAN TEMPLATE

Security Management Plan Template

1 Executive Summary

<This section should contain a brief summary of the business context of the system, any key IA controls, the assurance work done, any off-shoring considerations and any significant residual risks that need acceptance.>

2 System Description

2.1 Background

< A short description of the project/product/system. Describe its purpose, functionality, aim and scope.>

2.2 Organisational Ownership/Structure

<Who owns the system and operates the system and the organisational governance structure. This should include how any ongoing security management is integrated into the project governance e.g. how a Security Working Group reports to the project board.>

2.3 Information assets and flows

<The information assets processed by the system which should include a simple high level diagram on one page. Data flow diagram. Include a list of the type and volumes of data that will be processed, managed and stored within the supplier system. If personal data, please include the fields used such as name, address, department DOB, NI number etc.>

2.4 System Architecture

<A description of the physical system architecture, to include the system management. A diagram will be needed here>

2.5 Users

<A brief description of the system users, to include HMG users as well as any service provider users and system managers. If relevant, security clearance level requirements should be included.>

2.6 Locations

<Where the data assets are stored and managed from. If any locations hold independent security certifications (e.g. ISO27001 (at least ISO/IEC 27001:2013) these should be noted. Any off-shoring considerations should be detailed.>

2.7 Test and Development Systems

<Include information about any test and development systems, their locations and whether they contain live system data.>

2.8 Key roles and responsibilities

<A brief description of the lead security roles such as that of the SIRO, IAO, Security manager, Accreditor >

3 Risk Assessment

3.1 Assurance Scope

<This section describes the scope of the Assurance for the system. The scope of the assurance assessment should be clearly indicated, with components of the architecture upon which reliance is placed but assurance will not be done clearly shown e.g. a cloud hosting service. A logical diagram should be used along with a brief description of the components.>

3.2 Risk appetite

<A risk appetite should be agreed with the SRO and included here.>

3.3 Business impact assessment

< A description of the information assets and the impact of their loss or corruption (e.g. large amounts of Official Sensitive personal data the loss of which would be severely damaging to individuals, embarrassing to HMG, and make HMG liable to ICO investigations) in business terms should be included. This section should cover the impact on loss of confidentiality, integrity and availability of the assets. The format of this assessment may be dependent on the risk assessment method chosen.>

3.4 Risk assessment

<The content of this section will depend on the risk assessment methodology chosen and should contain the output of the formal information risk assessment in a prioritised list using business language. Experts on the system and business process should have been involved in the risk assessment to ensure the formal risk methodology used has not missed out any risks. The example table below should be used as the format to identify the risks and document the controls used to mitigate those risks. >

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
R1	Internet attackers could hack the system.	Medium	The service systems are exposed to the internet via the web portal.	C1: Internet-facing firewalls C2: Internet-facing IP whitelist C3: System hardening C4: Protective monitoring C5: Application access control C16: Anti-virus for incoming files C54: Files deleted when processed C59: Removal of departmental identifier	Very low
R2	Remote attackers could intercept or disrupt information crossing the internet.	Medium	File sharing with organisations across the internet.	C9: TLS communications C10: PGP file-sharing	Very low
R3	Internal users could maliciously or accidentally alter bank details.	Medium-High	Users bank details can be altered as part of the normal business function.	C12. System administrators hold SC clearance. C13. All changes to user information are	Low

Risk ID	Inherent risk	Inherent risk level	Vulnerability	Controls	Residual risk level
				logged and audited. C14. Letters are automatically sent to users' home addresses when bank details are altered. C15. Staff awareness training	

3.5 Controls

<The controls listed above to mitigate the risks identified should be detailed. There should be a description of each control, further information and configuration details where relevant, and an assessment of the implementation status of, and assurance in, the control. A sample layout is included below.>

ID	Control title	Control description	Further information and assurance status
C1	Internet-facing firewalls	Internet-facing firewalls are in place between the internet and the system', which restrict access from the internet to the required ports only.	Assured via ITHC firewall rule check
C2	Internet-facing IP whitelist	An IP whitelist is in place for all access from the internet.	Assured via ITHC
C15	Staff awareness training	All Staff must undertake annual security awareness training and this process is audited and monitored by line managers.	Assured as part of ISO/IEC 27001 (at least ISO/IEC 27001:2013) certification

3.6 Residual risks and actions

<A summary of the residual risks which are likely to be above the risk appetite stated after all controls have been applied and verified should be listed with actions and timescales included.>

4 In-service controls

< This section should describe the controls relating to the information lifecycle, including development, testing, in-service, termination and on-going risk management and accreditation assurance. Details of any formal assurance requirements specified in the contract such as security CHECK testing or maintained ISO/IEC 27001 (at least ISO/IEC 27001:2022) certification should be included. This section should include at least:

(a) information risk management and timescales and triggers for a review;

(b) contractual patching requirements and timescales for the different priorities of patch;

(c) protective monitoring arrangements to include how anomalous behaviour is identified and acted upon as well as how logging and auditing of user activity is done;

(d) configuration and change management;

(e) incident management;

(f) vulnerability management;

(g) user access management; and

(h) data sanitisation and disposal.>

5 Security Operating Procedures (SyOPs)

< If needed any SyOps requirements should be included and referenced here.>

6 Major Hardware and Software and end of support dates

< This should be a table which lists the end of support dates for hardware and software products and components. An example table is shown below.>

Name	Version	End of mainstream Support/Extended Support	Notes/RAG Status
Server Host	HP XXXX	Feb 2020/ March 2022	

7 Incident Management Process

<The suppliers' process, as agreed with the Authority/Customer, should be included here. It must as a minimum include the protocol for how and when incidents will be reported to the Authority/customer and the process that will be undertaken to mitigate the incidents and investigate the root cause.>

8 Security Requirements for User Organisations

<Any security requirements for connecting organisations or departments should be included or referenced here.>

9 Required Changes Register

<The table below shows the headings for the Required Changes Register which should be maintained and used to update the contents of this document at least annually.>

Ref	Section	Change	Agreed With	Date agreed	Documentation update	Status
1	6.4	A new Third Party supplier XXXX will be performing the print capability.	Authority name	11/11/2018	Jul-2019	Open

10 Sub-Contractors

<This should include a table which shows for each Sub-contractor their name, the function that they are performing, the data and data volume being processed, the location, and their certification status>

11 Annex A. ISO/IEC 27001 or later (at least ISO/IEC 27001:2022) and/or Cyber Essential Plus certificates

<Any certifications relied upon should have their certificates included>

12 Annex B. Cloud Security Principles assessment

<A spreadsheet may be attached>

13 Annex C. Protecting Bulk Data assessment if required by the Authority/Customer

<A spreadsheet may be attached>

14 Annex D. Latest ITHC report and Remediation Plan

SCHEDULE 7 – SECURE ESTABLISHMENTS

1. INTRODUCTION

1.1 The Authority has procured through this Contract the Supplier to provide the Services to a total of up to:

918 Children and Young People in youth custody in England and in Wales.

1.2 This Schedule lists those Secure Establishments within scope for the Supplier delivery of the Services to Children and Young People.

1.3 This Schedule also provides the units at each Secure Establishment relevant to the Unit Visits required as part of the Services, as set out in the service requirements section of the Specification and at CDI 3 in Annex A of Schedule 10 (Performance Mechanism).

Note: at most Secure Establishments, the number of beds exceeds the number of Children and Young People *in relation to which the Services are procured (as set out in Paragraph 2.1 below). Secure Establishments will use their available capacity to manage* Children and Young People *placed there.*

2. SECURE ESTABLISHMENTS

2.1 The Supplier shall provide the Services to Children and Young People at the following Secure Establishments:

Name	Advocacy Services Total Children and Young People
HM Young Offender Institute Cookham Wood	**188**
HM Young Offender Institute Feltham (A)	**150**
Oakhill Secure Training Centre	**80**
HM Prison & Young Offender Institute Parc – Young Person's Unit	**46**
HM Young Offender Institute Werrington	**118**
HM Young Offender Institute Wetherby	**336**
Total	**918**

2.2 The Supplier shall carry out Unit Visits at each Secure Establishment in respect of the following units in accordance with the Specification and CDI 3 in Annex A of Schedule 10:

Name	Provider	Capacity (Child or Young Person beds)	Sex
HM Young Offender Institute Cookham Wood Rochester, Kent, ME1 3LU	HMPPS	*Total* = **188**	M
Children & Young People Residential Units:			
A Block		90	M
B Block		89	M
Cedar House		17	M
Additional Units – not included in total capacity:			
x1 Care & Separation Unit			M
x1 Healthcare Unit			M
*Total Number of units within scope for **Unit Visits**:*		***5***	

Name	Provider	Capacity (Child or Young Person beds)	Sex
HM Young Offender Institute Feltham (A) Bedfont Road, Feltham, Middlesex, TW13 4ND	HMPPS	*Total* = **150**	M
Children & Young People Residential Units:			
Curlew (Induction) Unit		30	M
Dunlin Unit		30	M
Eagle Unit		30	M
Falcon Unit		30	M
Heron Unit		30	M
Jay Unit		30	M
Additional Units – not included in total capacity:			
x1 Care & Separation Unit			M
x1 Healthcare Unit			M
Alpine (Enhanced Support) Uni		(30)	M
*Total Number of units within scope for **Unit Visits**:*		***9***	

Name	Provider	Capacity (Child or Young Person beds)	Sex
Oakhill Secure Training Centre Chalgrove Field, Oakhill, Milton Keynes, MK5 6AJ	G4S	*Total =* **80**	M / F
Children & Young People Residential Units:			
	Ash 1	8	M
	Ash 2	8	M
	Ash 3	8	M
	Ash 4	8	M
	Willow 1 (Induction)	8	M
	Willow 2	8	M
	Willow 3	8	M
	Willow 4	8	M
	Oak 1	8	F
	Oak 2	8	F
Additional Units – not included in total capacity:			
	x1 Healthcare Unit	(4)	M / F
*Total Number of units within scope for **Unit Visits**:*		***11***	

Name	Provider	Capacity (Child or Young Person beds)	Sex
HM Prison & Young Offender Institute Parc – Young People's Unit Heol Hopcyn John, Bridgend, South Wales, CF35 6AP	G4S	*Total =* **46**	M
Children & Young People Residential Units:			
	Echo One	22	M
	Golf One	24	M

Additional Units – not included in total capacity:		
x1 Care & Separation Unit		M
x1 Healthcare Unit		M
*Total Number of units within scope for **Unit Visits**:*	***4***	

Name	**Provider**	**Capacity (Child or Young Person beds)**	**Sex**
HM Young Offender Institute Werrington Werrington, Stoke-On-Trent, ST9 0DX	HMPPS	*Total =* **188**	M
Children & Young People Residential Units:			
Doulton (A wing)		52	M
Doulton (B Wing)		44	M
Denby (Induction)		22	M
Additional Units – not included in total capacity:			
x1 Care & Separation Unit			M
x1 Healthcare Unit			M
Wade (Support) Unit		(8)	M
*Total Number of units within scope for **Unit Visits**:*		***6***	

Name	**Provider**	**Capacity (Child or Young Person beds)**	**Sex**
HM Young Offender Institute Wetherby York Road, Wetherby, West Yorkshire, LS22 5ED	HMPPS	*Total =* **336**	M / F
Children & Young People Residential Units:			
(Anson Unit)		(60)	
Benbow (First Night / Induction) Unit		48	M
Drake Wing		60	M
Exmouth Unit		60	M
Frobisher		60	M
Keppel (Complex Needs) Unit		48	M / F
Additional Units – not included in total capacity:			
x1 Care & Separation (on Anson) Unit		(15)	M / F

x1 Healthcare Unit		M / F
Napier (Enhanced Support) Unit	(8)	M / F
*Total Number of units within scope for **Unit Visits**:*	***8***	

2.3 Where the Authority agrees with a Secure Establishment the use of additional residential units but within the overall site total capacities – as given above – the Supplier shall continue to provide Advocacy Services to Children and Young People at no additional cost.

The Supplier is responsible for identifying and notifying to the Authority any impact on Services in the above instance.

3. ALTERNATIVE SECURE ESTABLISHMENTS

3.1 The Authority may, over the lifetime of this Contract, decide to decommission any of these Secure Establishments for use by Children and Young People – for example, where the population falls and accommodation is not required, or new accommodation comes online. In such circumstance, the Authority shall issue an Establishment Service Cessation Notice in accordance with Clause C4.

Such a decision would include the requisite adjustment to cease provision of the Services to Children and Young People at that/ those Secure Establishment/s, calculated in accordance with Clause C4 (Establishment Service Cessation Deduction).

3.2 In the above circumstance, it may also be that the Authority's decision includes placing Children and Young People into an alternative secure establishment (STC or YOI) to those listed in this Schedule.

3.3 Where providing Services to a number of Children and Young People at an alternative secure establishment that is still within the overall total number of Children and Young People given at Paragraph 1.1 above, the Authority may request for the Supplier to cost and deliver such Services, such costing to be proportionate to the Fixed Fees set out in the Fees Template and in accordance with any costing principles set out in the Fees Template.

3.4 The Authority will use the Change control mechanism at Schedule 3 to agree and formalise with the Supplier any such use of any and each alternative secure establishment/s.

SCHEDULE 8 – STATUTORY OBLIGATIONS AND CORPORATE SOCIAL RESPONSIBILITY

1 What the Authority expects from the Supplier

1.1 His Majesty's Government's Supplier Code of Conduct (the "**Code**") sets out the standards and behaviours expected of suppliers who work with government. The Code can be found online at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779660/20190220-Supplier_Code_of_Conduct.pdf

1.1 The Supplier shall, and shall procure that its Sub-Contractors shall:

1.1.1 comply with its legal obligations, in particular those in Part 1 of this Schedule 8, and meet the standards set out in the Code as a minimum; and

1.1.2 use reasonable endeavours to comply with the standards in Part 2 of this Schedule 8.

PART 1 Statutory Obligations

2 Equality and Accessibility

2.1 The Supplier shall:

(a) perform its obligations under this Contract in accordance with:

i) all applicable equality Law (whether in relation to race, sex, gender reassignment, age, disability, sexual orientation, religion or belief, pregnancy maternity or otherwise);

ii) the Authority's equality, diversity and inclusion policy as given to the Supplier from time to time; and

iii) any other requirements and instructions which the Authority reasonably imposes regarding any equality obligations imposed on the Authority at any time under applicable equality law.

(b) take all necessary steps and inform the Authority of the steps taken to prevent unlawful discrimination designated as such by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation).

3 Modern Slavery

3.1 The Supplier shall:

(a) not use, or allow Sub-Contractors to use, forced, bonded or involuntary prison labour;

(b) not require any Staff to lodge deposits or identity papers with their employer;

(c) allow, and ensure that any Sub-Contractors allow, Staff to leave their employer after reasonable notice;

(d) make reasonable enquiries to ensure that its Staff and Sub-Contractors have not been convicted of slavery or human trafficking offences anywhere in the world;

(e) have and maintain throughout the Term its own policies and procedures to ensure its compliance with the MSA and include in its Sub-Contracts anti-slavery and human trafficking provisions;

(f) not use, or allow its Staff to use physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation of its Staff and Sub-Contractors;

(g) not use or allow to be used child or slave labour to be used by its Sub-Contractors;

(h) if either Party identifies any occurrence of modern slavery in connection with this Contract, comply with the rectification process set out in clauses F2.4 to F2.6;

(i) prepare and deliver to the Authority each year, an annual slavery and trafficking report setting out the steps it has taken to ensure that slavery and trafficking is not taking place in any of its supply chains or in any part of its business;

(j) maintain a complete set of records to trace the supply chain of all Services provided to the Authority in connection with this Contract;

(k) report the discovery or suspicion of any slavery or trafficking by it or its Sub-Contractors to the Authority and to the Modern Slavery Helpline and other relevant national or local law enforcement agencies; and

(l) implement a system of training for its employees to ensure compliance with the MSA.

3.2 The Supplier represents, warrants and undertakes throughout the Term that:

(a) it has not been convicted of any slavery or human trafficking offences anywhere in the world; and

(b) to the best of its knowledge it is not currently under investigation, inquiry or enforcement proceedings in relation to any allegation of slavery or human trafficking offences anywhere in the world.

3.3 If the Supplier notifies the Authority pursuant to paragraph 3.1(i) of this Schedule 8, it shall respond promptly to the Authority's enquiries, co-operate with any

investigation, and allow the Authority to audit any books, records and/or any other relevant documentation in accordance with this Contract.

3.4 If the Supplier is in Default under paragraphs 3.1 or 3.2 of this Schedule 8 the Authority may by notice:

(a) require the Supplier to remove from performance of this Contract any Sub-Contractor, Staff or other persons associated with it whose acts or omissions have caused the Default; or

(b) immediately terminate this Contract.

4 Income Security

4.1 The Supplier shall:

(a) ensure that all pay and benefits paid for a standard working week meet, at least, national legal standards in the country of employment;

(b) provide all Staff with written and readily understandable information about their employment conditions in respect of pay before they enter employment and about their pay for the pay period concerned each time that they are paid;

(c) not make deductions from pay:

(ii) as a disciplinary measure;

(iii) except where permitted by Law and the terms of the employment contract; and

(iv) without express permission of the person concerned

(d) record all disciplinary measures taken against Staff.

5 Working Hours

5.1 The Supplier shall ensure that:

(a) the working hours of Staff comply with the Law, and any collective agreements;

(b) the working hours of Staff, excluding overtime, is defined by contract, do not exceed 48 hours per week unless the individual has agreed in writing, and that any such agreement is in accordance with the Law;

(c) overtime is used responsibly, considering:

(i) the extent;

(ii) frequency; and

(iii) hours worked;

(d) the total hours worked in any seven-day period shall not exceed 60 hours, except where covered by paragraph 5.1 (e);

(e) working hours do not exceed 60 hours in any seven-day period unless:

(iv) it is allowed by Law;

(v) it is allowed by a collective agreement freely negotiated with a worker's organisation representing a significant portion of the workforce;

(vi) appropriate safeguards are taken to protect the workers' health and safety; and

(vii) the Supplier can demonstrate that exceptional circumstances apply such as during unexpected production peaks, accidents or emergencies;

(f) all Supplier Staff are provided with at least:

(i) 1 day off in every 7-day period; or

(ii) where allowed by Law, 2 days off in every 14-day period.

6 Right to Work

6.1 The Supplier shall:

(a) ensure that all Staff, are employed on the condition that they are permitted to work in the UK, and;

(b) notify the authority immediately if an employee is not permitted to work in the UK.

7 Health and Safety

7.1 The Supplier shall perform its obligations under this Contract in accordance with:

(a) all applicable Law regarding health and safety; and

(b) the Authority's Health and Safety Policy while at the Authority's Premises.

7.2 Each Party shall notify the other as soon as practicable of any health and safety incidents or material health and safety hazards at the Authority's Premises of which it becomes aware and which relate to or arise in connection with the performance of this Contract. The Supplier shall instruct Staff to adopt any necessary safety measures in order to manage the risk.

8. Welsh Language Requirements

8.1 The Supplier shall comply with the Welsh Language Act 1993 and the Welsh Language Scheme as if it were the Authority to the extent that the same relate to the provision of the Services.

9 Fraud and Bribery

9.1 The Supplier represents and warrants that neither it, nor to the best of its knowledge any Staff, have at any time prior to the Commencement Date:

(a) committed a Prohibited Act or been formally notified that it is subject to an investigation or prosecution which relates to an alleged Prohibited Act; and/or

(b) been listed by any Government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in Government procurement programmes or contracts on the grounds of a Prohibited Act.

9.2 The Supplier shall not during the Term:

(a) commit a Prohibited Act; and/or

(b) do or suffer anything to be done which would cause the Authority or any of its employees, consultants, contractors, sub-contractors or agents to contravene any of the Relevant Requirements or otherwise incur any liability in relation to the Relevant Requirements.

9.3 The Supplier shall, during the Term:

(a) establish, maintain and enforce, and require that its Sub-Contractors establish, maintain and enforce, policies and procedures which are adequate to ensure compliance with the Relevant Requirements and prevent the occurrence of a Prohibited Act;

(b) have in place reasonable prevention measures (as defined in section 45(3) and 46(4) of the Criminal Finance Act 2017) to ensure that Associated Persons of the Supplier do not commit tax evasion facilitation offences as defined under that Act;

(c) keep appropriate records of its compliance with its obligations under paragraph 9.3 (a) and 9.3 (b) and make such records available to the Authority on request; and

(d) take account of any guidance about preventing facilitation of tax evasion offences which may be published and updated in accordance with section 47 of the Criminal Finances Act 2017.

9.4 The Supplier shall immediately notify the Authority in writing if it becomes aware of any breach of paragraphs 9.1 and/or 9.2, or has reason to believe that it has or any of the Staff have:

(a) been subject to an investigation or prosecution which relates to an alleged Prohibited Act;

(b) been listed by any Government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in Government procurement programmes or contracts on the grounds of a Prohibited Act; and/or

(c) received a request or demand for any undue financial or other advantage of any kind in connection with the performance of this Contract or otherwise suspects that any person directly or indirectly connected with this Contract has committed or attempted to commit a Prohibited Act.

9.5 If the Supplier notifies the Authority pursuant to paragraph 9.4, the Supplier shall respond promptly to the Authority's enquiries, co-operate with any investigation, and allow the Authority to Audit any books, records and/or any other relevant documentation.

9.6 If the Supplier is in Default under paragraphs 9.1 and/or 9.2, the Authority may by notice:

(a) require the Supplier to remove from performance of this Contract any Staff whose acts or omissions have caused the Default; or

(b) immediately terminate this Contract.

9.7 Any notice served by the Authority under paragraph 9.6 shall specify the nature of the Prohibited Act, the identity of the party who the Authority believes has committed the Prohibited Act and the action that the Authority has taken (including, where relevant, the date on which this Contract terminates).

PART 2 Corporate Social Responsibility

10 Zero Hours Contracts

10.1 Any reference to zero hours contracts, for the purposes of this Contract, means as they relate to employees or workers and not those who are genuinely self-employed and undertaking work on a zero hours arrangement.

10.2 When offering zero hours contracts, the Supplier shall consider and be clear in its communications with its employees and workers about:

(a) whether an individual is an employee or worker and what statutory and other rights they have;

(b) the process by which work will be offered and assurance that they are not obliged to accept work on every occasion; and

(c) how the individual's contract will terminate, for example, at the end of each work task or with notice given by either party.

11 Sustainability

11.1 The Supplier shall:

(a) comply with the applicable Government Buying Standards;

(b) provide, from time to time, in a format reasonably required by the Authority, reports on the environmental effects of providing the Goods and Services;

(c) maintain ISO 14001 or BS 8555 or an equivalent standard intended to manage its environmental responsibilities; and

(b) perform its obligations under this Contract in a way that:

(i) supports the Authority's achievement of the Greening Government Commitments;

(ii) conserves energy, water, wood, paper and other resources;

(iii) reduces waste and avoids the use of ozone depleting substances; and

(iv) minimises the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment.

SCHEDULE 9 – DATA PROCESSING

The Parties agree that this Schedule 9 will be discussed and finalised during the mobilisation phase of the Agreement.

1. The contact details of the Authority's Data Protection Officer are: data.compliance@justice.gov.uk ***or*** Data Protection Officer, 102 Petty France, London, SW1H 9AJ.

2. The contact details of the Supplier's Data Protection Officer are: [tbc].

3. For the purposes of Processing Personal Data under this Contract, the following circumstances are envisaged:

   (a) Processing by the Supplier as a Processor on behalf of the Authority as Controller,
   (b) Processing by the Parties as independent Controller,
   (c) Processing by the Parties as joint Controllers,

4. The ROPA described in Annex 2 of this Schedule 9 (Processing Personal Data) shall set out the record of processing activities under this Contract and shall indicate which scenario noted in paragraph 3 above shall apply in each situation.

Annex 1 – Joint Controllership

1. **Joint Controller Status and Allocation of Responsibilities**

1.1 If and to the extent that the Parties are Processing Personal Data under this Contract as joint Controllers, each Party undertakes to comply with the below obligations as set out in this Annex 1 and in compliance with the Data Protection Law in respect of their Processing of such Personal Data as joint Controllers.

1.2 The Parties agree that the [Supplier/Authority – tbc]:

(a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;

(b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

(c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;

(d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing or is otherwise necessary in accordance with Data Protection Law; and

(e) shall make available to Data Subjects the essence of this Annex 1 (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [Supplier's/Authority's - tbc] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of paragraph 1.2 above, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Law as against the relevant Party as Controller.

2. **Undertakings of both Parties**

2.1 The Supplier and the Authority each undertake that they shall:

(a) report to the other Party every [x - tbc] months on:

(i) the volume of Data Subject Requests (or purported Data Subject Requests) from Data Subjects (or third parties on their behalf);

(ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

(iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Law;

(iv) any communications from the ICO or any other regulatory authority in connection with Personal Data; and

(v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law,

that it has received in relation to the subject matter of this Contract during that period;

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in paragraphs 2.1(a)(i) to (v) above;

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in paragraphs 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Law;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, save where such disclosure or transfer is specifically authorised under this Contract or is required by Law). For the avoidance of doubt any third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex 1;

(e) request from the Data Subject only the minimum information necessary to provide the Services and treat such information as Confidential Information;

(f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

(g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

(i) are aware of and comply with their duties under this Annex 1 and those in respect of Confidential Information

(ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where that Party would not be permitted to do so;

(iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Law;

(h) ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data;

(i) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Law, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds; and

(i) ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

2.2 Each joint Controller shall use its reasonable endeavours to assist the other joint Controller to comply with any obligations under applicable Data Protection Law and shall not perform its obligations under this Annex 1 in such a way as to cause the other joint Controller to breach any of its obligations under applicable Data Protection Law to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations.

3. **Data Protection Breach**

3.1 Without prejudice to paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of

any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, including the following:

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Law;

(b) all reasonable assistance, including:

(i) co-operation with the other Party and the ICO investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

(ii) co-operation with the other Party including taking such reasonable steps as are directed by the Authority to assist in the investigation, mitigation and remediation of a Personal Data Breach;

(iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or

(iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the ICO investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in paragraph 3.2.

3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has been lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach, as if it were that Party's own data. Such steps shall be taken at that Party's own cost and with all possible speed. That Party shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach, all relevant information relating to the Personal Data Breach, in particular:

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

(c) the categories and number of Data Subjects concerned;

(d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

(e) measures taken or proposed to be taken to address the Personal Data Breach; and

(f) describe the likely consequences of the Personal Data Breach.

4. **Audit**

4.1 The Supplier shall permit:

(a) the Authority, or a third-party auditor acting under the Authority's direction, to conduct, at the Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 1 and the Data Protection Law; and/or

(b) the Authority, or a third-party auditor acting under the Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to this Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

4.2 The Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with paragraph 4.1 in lieu of conducting such an audit, assessment or inspection.

5. **DPIAs**

5.1 The Parties shall:

(a) provide all reasonable assistance to each other to prepare any DPIAs as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

(b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with this Contract, in accordance with the terms of Article 30 of the UK GDPR.

6. **Termination**

6.1 If the Supplier is in material Default under any of its obligations under this Annex 1, the Authority shall be entitled to terminate this Contract in accordance with the provisions in clause H2 (Termination on Default).

7. **Sub-Processing**

7.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by this Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

(b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Law.

8. **Data Retention**

8.1 The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Law and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by this Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Law and its privacy policy. The Parties shall comply with Clause H9 of this Contract in relation to the deletion of Personal Data at the end of this Contract.

ANNEX 2 – SCHEDULE 9

References in this Schedule 9 to the **"ROPA"** mean the Excel spreadsheet entitled "BARNARDO'S/MOJ DATA FLOW TABLE AND ROPA" agreed between the Authority and the Supplier, as such document may be updated from time to time by written agreement between the Authority and the Supplier.

For the purposes of paragraph 3 of Schedule 9 above, the subject matter of the Processing is such Processing as is required to ensure that the Supplier can effectively deliver the Services under this Contract. Furthermore:

- The relationship between the Parties for each relevant Processing activity shall be as described in column H of the ROPA.
- The nature and purpose of the Processing for each relevant Processing activity shall be as described in column C of the ROPA.
- The categories of Personal Data for each relevant Processing activity shall be as described in column D of the ROPA.
- The categories of Data Subjects for each relevant Processing activity shall be as described in column G of the ROPA.
- The duration of the Processing for each relevant Processing activity shall be as described in column O of the ROPA.
- The location of the Personal Data for each relevant Processing activity shall be as described in column P of the ROPA.
- The security measures that the Supplier has in place shall be as described in column Q of the ROPA.

SCHEDULE 10- PERFORMANCE MECHANISM

1. Introduction

1.1 In order for the Authority to assure itself of the performance of this Contract, a range of different mechanisms, detailed in this Schedule 10, have been established for the Supplier to comply with. Each remedy shall be without prejudice to the Authority's other remedies, and may be applied independently on the terms set out in this Schedule 10.

1.2 The Supplier shall provide to the Authority performance information as detailed in this Schedule and under this Contract, together with any further performance information deemed necessary by the Authority.

1.3 Regardless of the information reporting detailed under this Contract and this Schedule 10, the Supplier shall provide a report immediately to the Authority detailing any issues of concern or matters which may become of ministerial interest or may have media interest upon becoming aware of such matters, or upon the Authority's request.

2. Contract Delivery Indicators

2.1 The Authority has identified a number of Contract Delivery Indicators (CDIs), listed at Annex A to this Schedule 10. The order in which the CDIs appear does not indicate relative priority.

2.2 The CDIs relate solely to the Supplier's performance in respect of the relevant obligations. Absence of a CDI for any other aspect of the Supplier's obligations under this Contract does not mean that the Supplier has no responsibility or liability for poor performance in those areas. Any poor performance gives rise to a requirement for improvement or Financial Remedy in accordance with paragraphs 5 to 8 below.

2.3 **Contract Delivery Indicators Review**

a) The Parties may (acting reasonably and in good faith) at the end of each Contract Year (or at such other point in time as may be agreed between the Parties) determine additional or amended CDIs to those set out in this Schedule 10 so as to reflect the standards of service required by the Authority, any such additional CDIs or amendments to the CDIs shall be implemented in accordance with Schedule 3 (Change Control). In the event that the Parties are unable to agree any such additional or amended CDIs, the matter shall be referred to the procedure set out in Clause I1 (Dispute Resolution).

b) 'Without prejudice to the generality of paragraph 2.3(a), the Authority may on giving the Supplier at least three (3) Months' notice vary the number of Performance Points applicable to each CDI. The Supplier shall not be entitled to object to any such change provided that the total number of Performance Points across all CDIs does not increase.

3. Performance Management Information

3.1 In order for the Authority to be able to assure the performance of the Supplier against its obligations, management information reports and data as set out below shall be provided by the Supplier to the Authority**:**

a) Monthly data returns, utilising the agreed reporting template provided by the Supplier and approved by the Authority during the Mobilisation Period (each a "**Monthly Data Return**") will be provided for each secure establishment within seven (7) calendar days following the Month end;

b) Quarterly contract management reports utilising the template provided by the Supplier and approved by the Authority during the Mobilisation Period (each a "**Quarterly Contract Management Report**") will be submitted to the Authority by the seventh (7th) calendar day after the end of each Performance Quarter, and shall include the Supplier's proposal for the improvement of the Services to address any thematic issues identified in respect of CDI performance that it not subject to an Improvement Plan;

c) An annual report for commissioners utilising the template provided by the Supplier and approved by the Authority during the Mobilisation Period with a further annexed report suitable for publishing (each an "**Annual Report**") will be submitted to the Authority within six (6) weeks after the end of each Contract Year, and a final report, based on feedback from the Authority, will be submitted within ten (10) weeks after the end of the Contract Year. The annex to the Annual Report should be jointly approved and mutually agreed in the event that either the Authority or Supplier wish to publish.

3.2 In addition to this performance information, the Supplier will be required to attend the following governance meetings as requested by the Authority from time to time:

Meeting	Attendees	Frequency
Advocacy Review Meetings (ARMs)	Supplier and Secure Establishment SLG.	At least once every month
OCM Service meetings	Supplier and YCS OCM.	At least once every month
Contract Review Meetings	Supplier and MoJ CCM, with YCS OCM.	At least once every Performance Quarter

Annual Service Review	Supplier and MoJ CCM, with YCS OCM.	Once every Contract Year

4. Performance Mechanism Remedies

4.1 Where the Performance Points Threshold and/or the Performance Mechanism Trigger is met in the relevant period, the following remedies shall be available to the Authority:

Ref	Authority Response Level	Performance Points Threshold		Performance Mechanism Trigger
1	**Performance Points award only (no action)**	In Contract Year 1: 0 – 119 Performance Points per Performance Quarter In Contract Year 2: 0 – 99 Performance Points per Performance Quarter In Contract Year 3 and each subsequent Contract Year: 0 – 79 Performance Points per Performance Quarter	**and/ or**	n/a
2	**Authority's right to reduce payment is triggered (Financial Remedy)**	In Contract Year 1: 120 Performance Points or more per Performance Quarter In Contract Year 2: 100 Performance Points or more per Performance Quarter In Contract Year 3 and each subsequent Contract Year: 80 Performance Points or more per Performance Quarter	**and/ or**	The Supplier fails to respond to an Outstanding Issues Notice or to remedy the issues identified in an Outstanding Issues Notice within the required timescales as per paragraph 7.3.

3	**Authority's right to terminate this Contract is triggered**	In Contract Year 1: 360 Performance Points or more per rolling 12-Month period In Contract Year 2: 400 Performance Points or more per rolling 12-Month period In Contract Year 3 and each subsequent Contract Year: 320 Performance Points or more per rolling 12-Month period	**and/ or**	The Supplier fails to deliver: (a) on any one or more Outstanding Issues Notice(s) on three (3) occasions in a rolling 12-Month period; or (b) on any one Outstanding Issues Notice for six (6) consecutive Months following the date on which the issue was due to have been rectified as set out in the Outstanding Issues Notice.

5. Improvement Notices

5.1 The Authority may issue a notice bringing this to the attention of the Supplier, if at any time the Authority considers in its reasonable opinion that the Supplier has demonstrated Reduced Performance (an "**Improvement Notice**").

5.2 The Authority may issue an Improvement Notice concerning any aspect of the provision of the Services whether or not these are related to CDIs.

5.3 An Improvement Notice shall state:

a) any area of Reduced Performance (which may include the nature and dates on which the occurrences of failure were recorded or took place); and

b) any other supporting information which the Authority considers to be relevant.

6. Improvement Plan

6.1 Within seven (7) Working Days of the date of issue of an Improvement Notice, the Supplier shall deliver to the Authority a plan (the "**Improvement Plan**") in respect of the areas of Reduced Performance identified in the Improvement Notice, which shall:

a) provide an explanation of the causes of the Reduced Performance;

b) identify the actions needed to remedy the Reduced Performance identified in the Improvement Notice and prevent its re-occurrence (the

"**Improvement Actions**");

c) set out:

(1) the Supplier's proposals for carrying out the Improvement Actions;

(2) a programme for undertaking such actions;

(3) the date by which such actions will be completed;

(4) any actions or consents required from the Authority to facilitate the Supplier's remedial actions; and

(5) specify proposed criteria for the purpose of auditing the completion of the remedial actions and resolution of the Reduced Performance.

6.2 Following receipt of an Improvement Plan, the Authority may (acting reasonably):

a) agree the Improvement Plan; or

b) reject the Improvement Plan and require the Supplier to submit a revised Improvement Plan or issue an Outstanding Issues Notice within seven (7) Working Days of such rejection (or such other time as may be agreed by the Parties in writing).

6.3 Each Improvement Plan shall be sequentially numbered from a central register maintained by the Authority. In the event that a further unconnected circumstance occurs which results in the issue of a separate Improvement Notice, a separate Improvement Plan shall be raised and recorded in the central register under a separate sequential number.

6.4 An Improvement Plan may relate to one or more incidents of Reduced Performance and to a particular Secure Establishment, a number of Secure Establishments, central functions, or the whole contract area.

6.5 The Supplier shall implement all the Improvement Actions by the date(s) specified in the Improvement Plan at no cost to the Authority. A failure to do so shall constitute a Material Breach.

6.6 An Improvement Plan shall remain open until the Improvement Actions identified therein have been completed in accordance with the agreed Improvement Plan to the Authority's satisfaction, whereupon it shall be closed.

6.7 A report on progress against each open Improvement Plan shall be provided at agreed intervals.

6.8 The Authority shall measure progress against an Improvement Plan by auditing the completion of Improvement Actions and requesting any information from the Supplier (which the Supplier shall promptly provide) as it reasonably

required to assure itself of completion.

7. Outstanding Issues Notice

7.1 Where the Supplier fails to submit a revised Improvement Plan, or the revised Improvement Plan is in the Authority's reasonable opinion unacceptable or where the Improvement Actions are carried out and completed but do not succeed in remedying the Reduced Performance identified in the Improvement Notice or in preventing its re-occurrence, the Authority may either:

a) issue a further Improvement Notice in respect of the same areas of poor performance; or

b) issue an Outstanding Issues Notice in accordance with this paragraph 7 ("**Outstanding Issues Notice**").

7.2 An Outstanding Issues Notice shall state:

a) any area of Reduced Performance (which may include the nature and dates on which the occurrences of failure were recorded or took place); and

b) any uncompleted Improvement Actions; and/or

c) the aspects in which the Improvement Plan is unacceptable,

and the Parties shall in good faith attempt to resolve such Outstanding Issues.

7.3 If:

a) the Parties fail to reach agreement in resolving the Outstanding Issues within fourteen (14) Working Days of the date of the Outstanding Issues Notice, or such other time as may be agreed by the Parties in writing; or

b) the Supplier fails to resolve the Outstanding Issues Notice within the timescales agreed therein,

the Authority reserves its right to seek financial remedy in accordance with paragraph 8.3 below.

8. Financial Remedy

8.1 Where the Performance Points Threshold or one of the Performance Mechanism Triggers has or have been met in accordance with row 2 of the table in paragraph 4.1 above, the Authority may issue a financial remedy representing a deduction to Fixed Fees calculated in accordance with paragraphs 8.2 to 8.4 below ("**Financial Remedy**") by bringing this to the attention of the Supplier.

8.2 The Financial Remedy shall scale between 0% and 5%, but shall not exceed 5%, of the total Fixed Fees payable in the relevant Performance Quarter. For the avoidance of doubt, where both the Performance Points Threshold and a Performance Mechanism Trigger are met, the maximum Financial Remedy in any Performance Quarter shall be 5% of the total Fixed Fees applicable to that Performance Quarter.

8.3 Where the Financial Remedy is applied as a result of the Performance Points Threshold being met, the Financial Remedy shall be calculated in accordance with this paragraph 8.3:

FR = (QFF x 5%) x ((TQPP – PPB) / 100)), where:

FR	=	the Financial Remedy
QFF	=	the total Fixed Fees attributable the relevant Performance Quarter
TQPP	=	Total Quarterly Performance Points, being the aggregate of the Performance Points accrued by the Supplier in the relevant Performance Quarter
PPB	=	Performance Points Baseline, being: in Contract Year 1: 120 Performance Points per Performance Quarter in Contract Year 2: 100 Performance Points per Performance Quarter in Contract Year 3 and each subsequent Contract Year: 100 Performance Points per Performance Quarter

8.4 Where the Financial Remedy is applied as a result of the Performance Mechanism Trigger being met, the Financial Remedy shall be calculated in accordance with this paragraph 8.4:

The Financial Remedy shall be a sum equal to 5% of the Fixed Fees in the Performance Quarter in which the Supplier's failure to respond to or remedy an Outstanding Issues Notice occurred.

8.5 Where the Authority notifies the Supplier that a Financial Remedy

shall be payable, the Supplier shall reduce the value of the invoice issued in the Month immediately following the end of the relevant Performance Quarter (or, at the Authority's discretion, any subsequent Month's invoice) by the value of the Financial Remedy, in accordance with paragraph 1.1 of Schedule 2 (Payment Mechanism).

8.6 Any Financial Remedy owing to the Authority at the end of the Term shall be calculated according to paragraph 8 and credited in the final invoice according to paragraph 8.3 above.

Annex A: CDIs

The following table sets out the Contract Delivery Indicators (CDIs).

The Authority may wish to publish performance information in respect of any of the CDIs given for this Contract. The final column of the table below shows those CDIs the Authority wishes to publish performance information for (and this shall be updated as required by the Authority in each subsequent Contract Year).

Ref	Contract Delivery Indicator (CDI)	Performance Points for failure	Publishable Performance Information *(yes / no)*
1	100% of Children and Young People **newly admitted** to the Secure Establishment will have an **introduction** to Advocacy Services at the Secure Establishment **within seven (7) calendar days** of their admission.	**10pts per failure**	yes
2	100% of Children and Young People **newly admitted** to the Secure Establishment will have a Children's & Human Rights **Awareness Session** as part of their Induction to the Secure Establishment within **fourteen (14) calendar days** of their admission.	**10pts per failure**	yes
3	The Supplier will undertake (at least the minimum) **Unit Visits** at each Secure Establishment **each calendar week**, as detailed in the Section 1 of the Specification.	**10pts per unit missed**	no
4	For any **request made** for an Advocate to contact a Child or Young Person, regardless of the referral source, the Advocate will 100% of the time engage the Child or Young Person **within 72 hours** (3 calendar days) of notification to offer them support.	**30pts per failure (+1pt for each subsequent day of failure)**	yes
5	For any **urgent request made** to an Advocate to contact a Child or Young Person, regardless of the referral source, the Advocate will engage the	**40pts per failure (+1pt for each**	no

	Child or Young Person **within 24 hours** (1 calendar day) of notification to offer them support.	**subsequent day of failure)**	
6	The Supplier shall comply with the performance management information **data reporting** requirements as stipulated at Paragraph 3 of this Schedule 10 (Performance Management) ***and*** any reasonable **request for information** made by the Authority in writing (including in relation to the Supplier's compliance with CDI 7 below) to the Supplier will be fulfilled by the Supplier by the deadline provided in said notice.	**5pt per failure**	no
7	The Supplier shall report to the Authority on at least a quarterly basis the total percentage of full-time equivalent (FTE) people from groups under-represented in the workforce employed under the Contract, as a proportion of the total FTE Contract workforce, by UK region.	**5pt per failure, under CDI 6**	no

SCHEDULE 11 – BUSINESS CONTINUITY PLAN

1 Definitions

1.1 In this Schedule, the following definitions shall apply:

"**Disaster**"	the occurrence of one or more events which, either separately or cumulatively, mean that the Services, or a material part of the Services will be unable to be delivered without the activation of bespoke continuity measures;
"**Disaster Recovery System**"	the system embodied in the processes and procedures for restoring the provision of Services following the occurrence of a Disaster;
"**Related Supplier**"	any person who provides services to the Authority in relation to this Contract from time to time.

2 Business Continuity Plan

2.1 The Business Continuity Plan shall:

2.1.1 be divided into four sections:

(a) Section 1 which shall set out general principles applicable to the Business Continuity Plan;

(b) Section 2 which shall relate to Business Continuity; and

(c) Section 3 which shall relate to Disaster Recovery.

2.1.2 unless otherwise required by the Authority in writing, be based upon and be consistent with the provisions of paragraphs 3, 4 and 5 below.

2.2 The Authority shall:

2.2.1 review and comment on the draft plan set out in Annex A of this Schedule 11 as soon as reasonably practicable following the Commencement Date;

2.2.2 notify the Supplier in writing that it approves or rejects the draft plan no later than twenty (20) Working Days after the Commencement Date.

2.3 If the Authority rejects the draft plan:

2.3.1 the Authority shall inform the Supplier in writing of its reasons for its rejection; and

2.3.2 the Supplier shall then revise the draft plan (taking reasonable account of the Authority's comments) and shall re-submit a revised draft plan to the Authority for the Authority's approval within ten (10) Working Days of the date of the Authority's notice of rejection. The provisions of paragraph 1.2 and this paragraph 1.3 shall apply again to any resubmitted draft plan, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.

3 SECTION 1 OF THE BUSINESS CONTINUITY PLAN – GENERAL PRINCIPLES

3.1 Section 1 of the Business Continuity Plan shall:

3.1.1 set out how the business continuity and disaster recovery elements of the Business Continuity Plan link to each other;

3.1.2 provide details of how the invocation of any element of the Business Continuity Plan may impact upon the provision of the Services and any goods and/or services provided to the Authority by a Related Supplier;

3.1.3 contain an obligation upon the Supplier to liaise with the Authority and any Related Suppliers with respect to business continuity and disaster recovery;

3.1.4 detail how the Business Continuity Plan interoperates with any overarching disaster recovery or business continuity plan of the Authority and any of its other Related Suppliers in each case as notified to the Supplier by the Authority from time to time;

3.1.5 contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multiple channels;

3.1.6 contain a risk analysis, including:

(a) failure or disruption scenarios and assessments of likely frequency of occurrence;

(b) identification of any single points of failure within the provision of Services and processes for managing those risks;

(c) identification of risks arising from the interaction of the provision of Services with the goods and/or services provided by a Related Supplier; and

(d) a business impact analysis of different anticipated failures or disruptions;

3.1.7 provide for documentation of processes, including business processes, and procedures;

3.1.8 set out key contact details for the Supplier (and any Sub-Contractors) and for the Authority;

3.1.9 identify the procedures for reverting to "normal service";

3.1.10 set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to minimise data loss;

3.1.11 identify the responsibilities (if any) that the Authority has agreed it will assume in the event of the invocation of the Business Continuity Plan; and

3.1.12 provide for the provision of technical assistance to key contacts at the Authority as required by the Authority to inform decisions in support of the Authority's business continuity plans.

3.2 The Business Continuity Plan shall be designed so as to ensure that:

3.2.1 the Services are provided in accordance with this Contract at all times during and after the invocation of the Business Continuity Plan;

3.2.2 the adverse impact of any disaster is minimised as far as reasonably possible;

3.2.3 it complies with the relevant provisions of ISO/IEC 27002 and all other industry standards from time to time in force; and

3.2.4 it details a process for the management of disaster recovery testing.

3.3 The Business Continuity Plan shall be upgradeable and sufficiently flexible to support any changes to the Services and the business operations supported by the provision of Services.

3.4 The Supplier shall not be entitled to any relief from its obligations under the CDIs or to any increase in the Price to the extent that a disaster occurs as a consequence of any breach by the Supplier of this Contract.

4 SECTION 2 OF THE BUSINESS CONTINUITY PLAN – BUSINESS CONTINUITY

4.1 Section 2 of the Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes facilitated by the provision of Services remain supported and to ensure continuity of the business operations supported by the Services including:

4.1.1 the alternative processes, options and responsibilities that may be adopted in the event of a failure in or disruption to the provision of Services; and

4.1.2 the steps to be taken by the Supplier upon resumption of the provision of Services in order to address the effect of the failure or disruption.

4.2 Section 2 of the Business Continuity Plan shall:

4.2.1 address the various possible levels of failures of or disruptions to the provision of Services;

4.2.2 set out the goods and/or services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Services (the "**Business Continuity Services**");

4.2.3 specify any applicable service levels or CDIs with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the CDIs in respect of the provision of other Services during any period of invocation of the Business Continuity Plan; and

4.2.4 set out the circumstances in which the Business Continuity Plan is invoked.

5 SECTION 3 OF THE BUSINESS CONTINUITY PLAN – DISASTER RECOVERY

5.1 Section 3 of the Business Continuity Plan shall be designed to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Authority supported by the Services following any disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.

5.2 Section 3 of the Business Continuity Plan shall include the following:

5.2.1 the design and build specification of the Disaster Recovery System;

5.2.2 details of the procedures and processes to be put in place by the Supplier in relation to the Disaster Recovery System and the provision of the Disaster Recovery Services and any testing of the same including:

(a) the process for conducting a business impact assessment to determine the acceptable length of time of non-availability;

(b) such procedures and processes as are required to ensure compliance with ISO 27001:2013;

(c) identification of all potential disaster scenarios;

(d) risk analysis;

(e) documentation of processes and procedures;

(f) invocation rules;

(g) service recovery procedures; and

(h) steps to be taken upon resumption of the provision of Services to address any prevailing effect of the failure or disruption of the provision of the Services;

5.2.3 any applicable service levels of CDIs with respect to the provision of the Disaster Recovery Services and details of any agreed relaxation to the CDIs in respect of the provision of other Services during any period of invocation of Section 3 of the Business Continuity Plan;

5.2.4 details of how the Supplier shall ensure compliance with security standards ensuring that compliance is maintained for any period during which Section 3 of the Business Continuity Plan is invoked;

5.2.5 access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and

5.2.6 testing and management arrangements.

6 Review and amendment of the Business Continuity Plan

6.1 The Supplier shall at its own cost review and update the Service Continuity Plan (and the risk analysis on which it is based):

6.1.1 on a regular basis and as a minimum once every twelve (12) Months;

6.1.2 within three (3) Months of the Business Continuity Plan (or any part) having been invoked pursuant to paragraph 8;

6.1.3 where the Authority requests any additional reviews (over and above those provided for in paragraphs 6.1.1 and 6.1.2) by notifying the Supplier to such effect in writing, whereupon the Supplier shall conduct such reviews in accordance with the Authority's written requirements.

6.2 Each review of the Business Continuity Plan pursuant to paragraph 6.1 shall be a review of the procedures and methodologies set out in the Business Continuity Plan and shall assess their suitability having regard to any change to the Services or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the Business Continuity Plan or the last review of the Business Continuity Plan and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the Business Continuity Plan. The review shall be completed by the Supplier within the period required by the Business Continuity Plan or, if no such period is required, within such period as the Authority shall reasonably require.

6.3 The Supplier shall, as soon as reasonably practicable following the completion of a review carried out in accordance with paragraphs 6.1 and 6.2, notify the Authority of the outcome of the review, including any issues or inadequacies identified in the Business Continuity Plan, its practices or procedures and shall submit for approval by the Authority any steps that the Supplier proposes to take in order to rectify such issues or inadequacies (as required by paragraph 6.4).

6.4 The Supplier shall in consultation with the Authority take all reasonable steps necessary to promptly rectify any issues or inadequacies identified in the Business Continuity Plan, its practices or procedures during a review carried

out in accordance with paragraphs 6.1 and 6.2, and shall notify the Authority once these have been resolved.

7 Testing of the Business Continuity Plan

7.1 The Supplier shall at its own cost test the Business Continuity Plan on a regular basis (and in any event not less than once in every Contract Year). Subject to Paragraph 7.2, the Authority may require the Supplier to conduct additional tests of some or all aspects of the Business Continuity Plan at any time where the Authority considers it necessary, including where there has been any change to the Services or any underlying business processes, or on the occurrence of any event which may increase the likelihood of the need to implement the Business Continuity Plan.

7.2 If the Authority requires an additional test of the Business Continuity Plan, it shall give the Supplier written notice and the Supplier shall conduct the test within thirty (30) days, in accordance with the Authority's requirements and the relevant provisions of the Business Continuity Plan.

7.3 The Supplier shall undertake and manage testing of the Business Continuity Plan in full consultation with the Authority and shall liaise with the Authority in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Authority in this regard.

7.4 The Supplier shall, as soon as reasonably practicable following the completion of a testing carried out in accordance with paragraphs 7.1 to 7.3, notify the Authority of the outcome of the testing, including any issues or inadequacies identified in the Business Continuity Plan, its practices or procedures and shall submit for approval by the Authority any steps that the Supplier proposes to take in order to rectify such issues or inadequacies (as required by paragraph 7.5).

7.5 The Supplier shall in consultation with the Authority take all reasonable steps necessary to promptly rectify any issues or inadequacies identified in the Business Continuity Plan, its practices or procedures during testing carried out in accordance with paragraphs 7.1 to 7.3, and shall notify the Authority once these have been resolved.

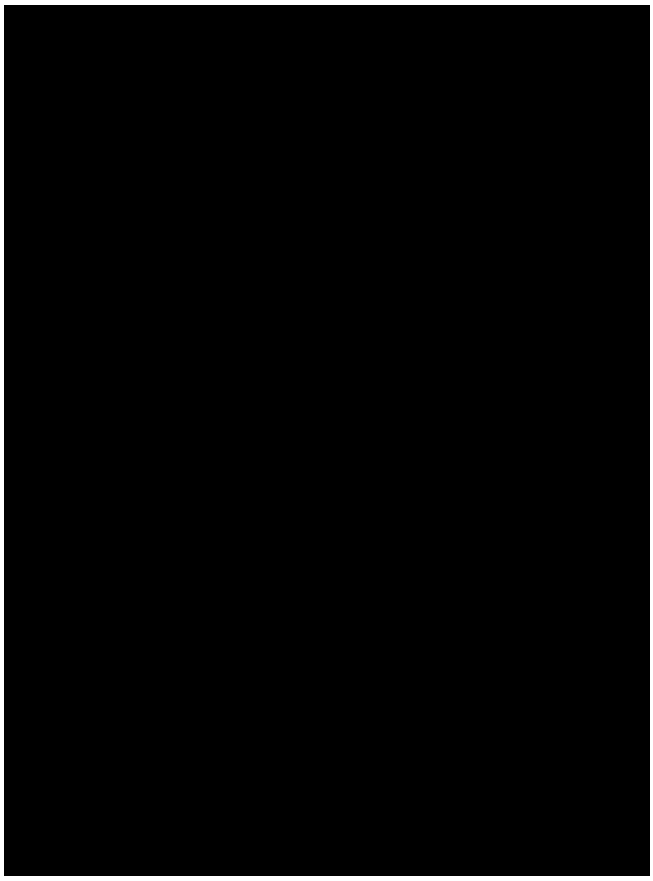
7.6 For the avoidance of doubt, the carrying out of a test of the Business Continuity Plan (including a test of the Business Continuity Plan's procedures) shall not relieve the Supplier of any of its obligations under this Contract.

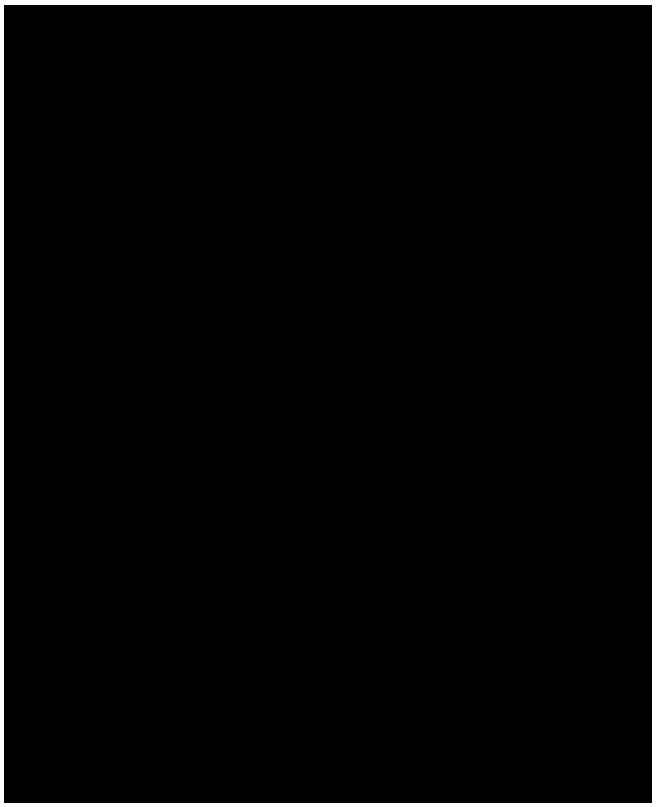
8 Invocation of the Business Continuity Plan

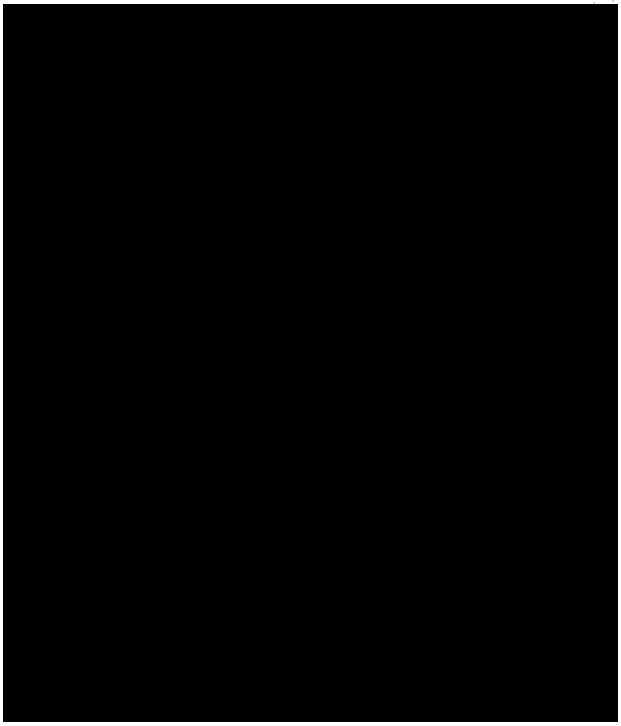
8.1 In the event of a loss of any critical part of the Service or a Disaster, the Supplier shall immediately invoke the business continuity and disaster recovery provisions in the Business Continuity Plan, including any linked

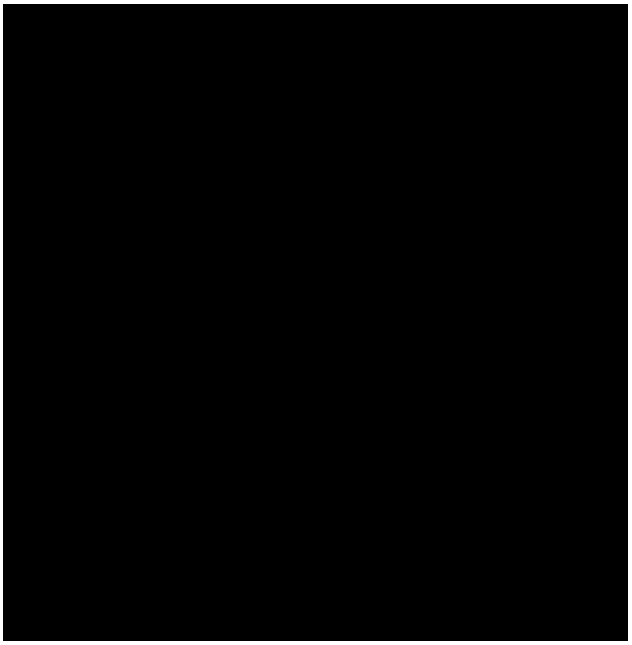
elements in other parts of the Business Continuity Plan, and shall inform the Authority promptly of such invocation. In all other instances the Supplier shall invoke the business continuity and disaster recovery elements in the Business Continuity Plan only with the prior consent of the Authority.

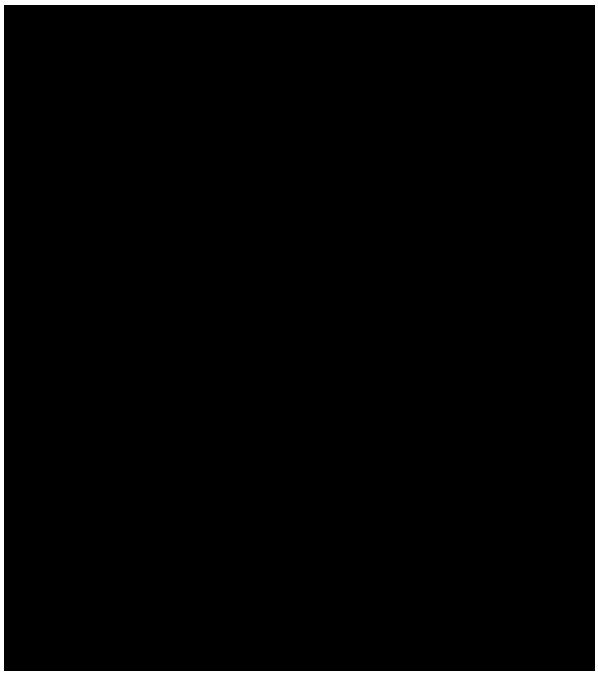
Annex A: Draft Business Continuity Plan

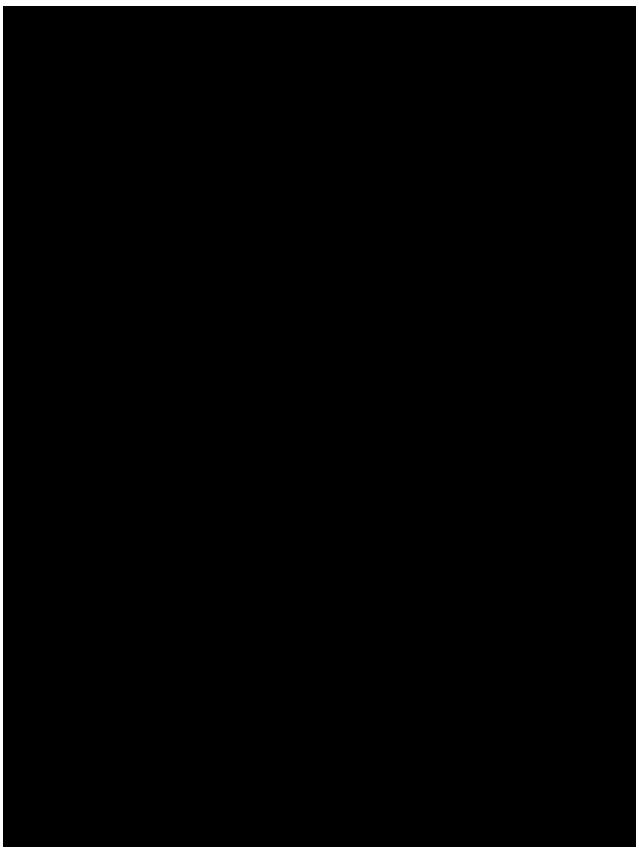


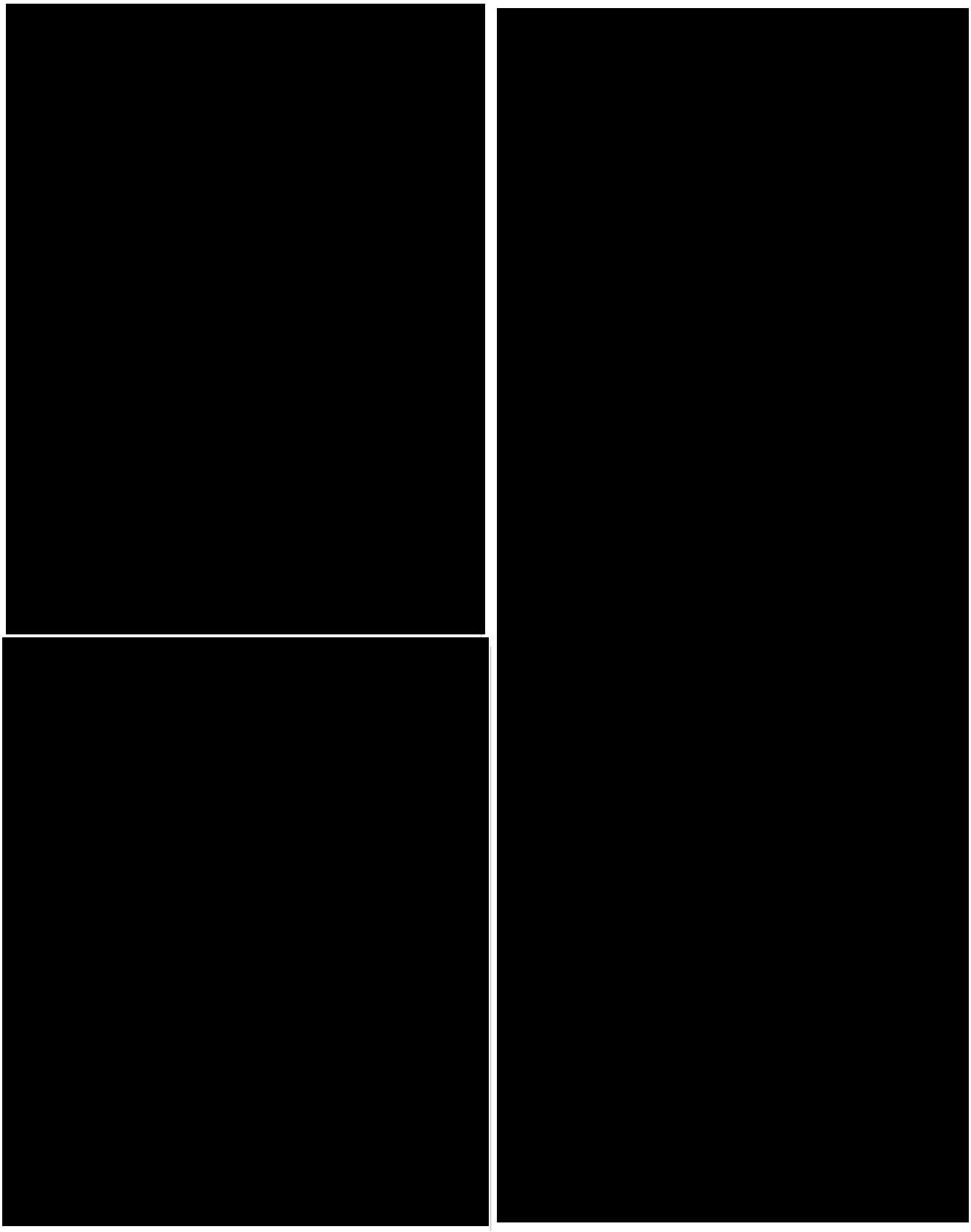


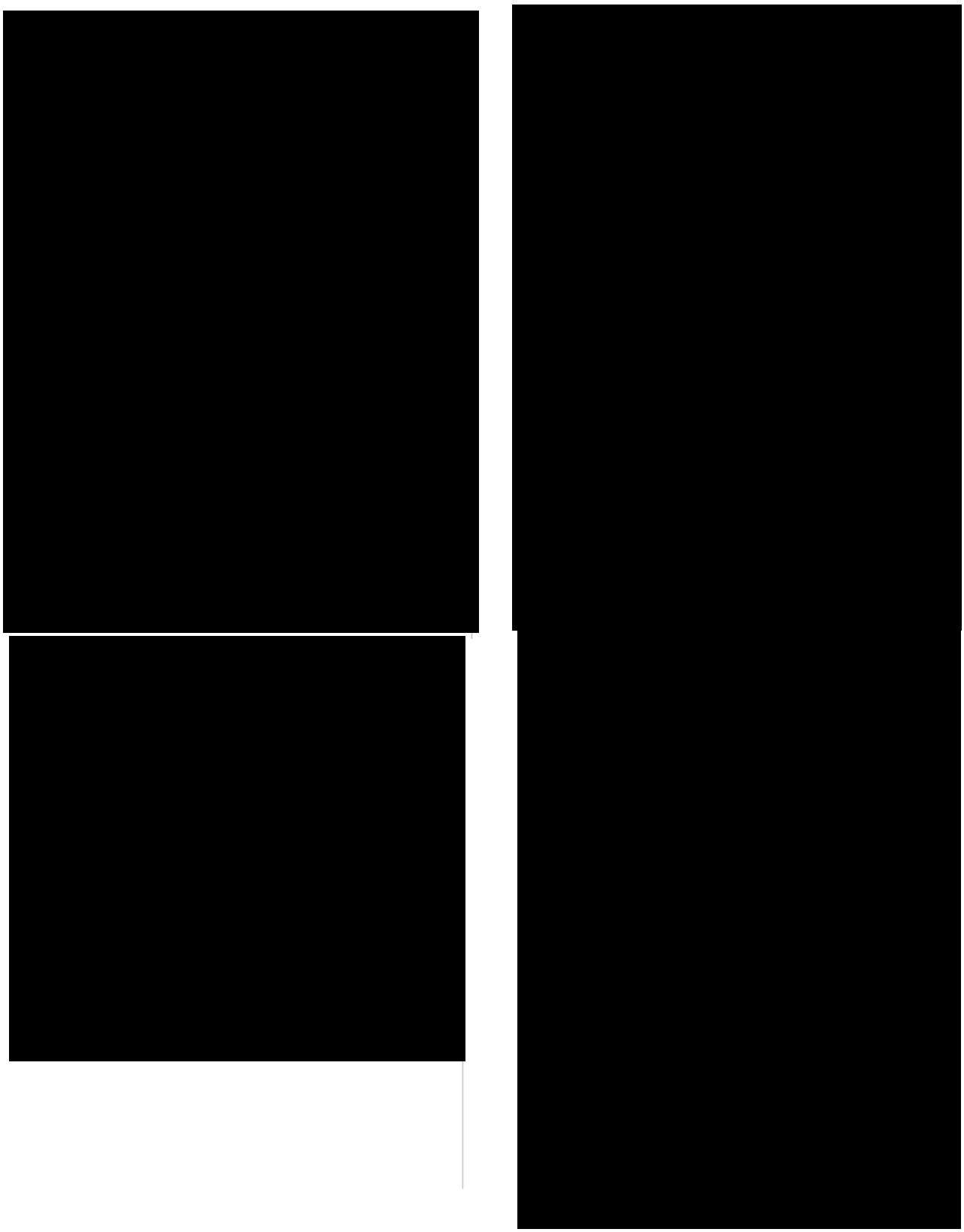


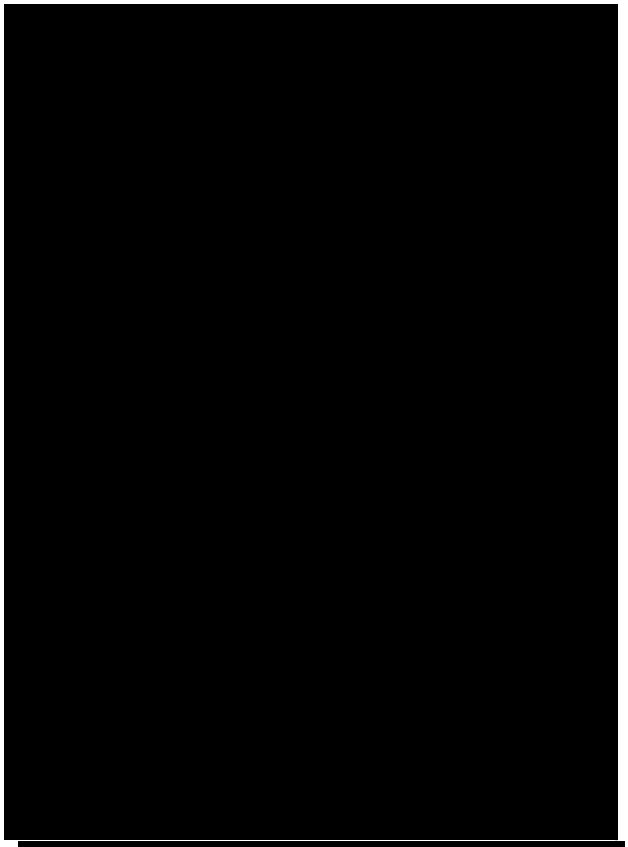


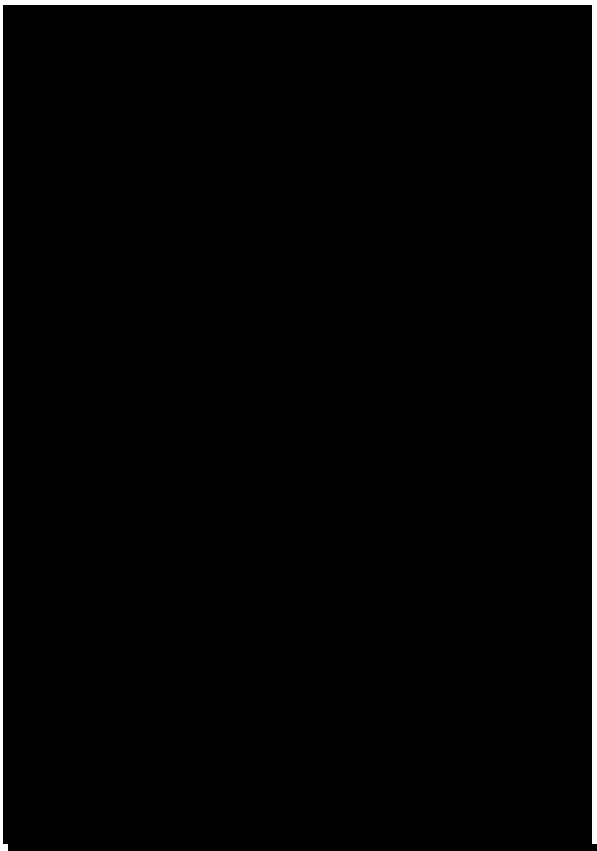


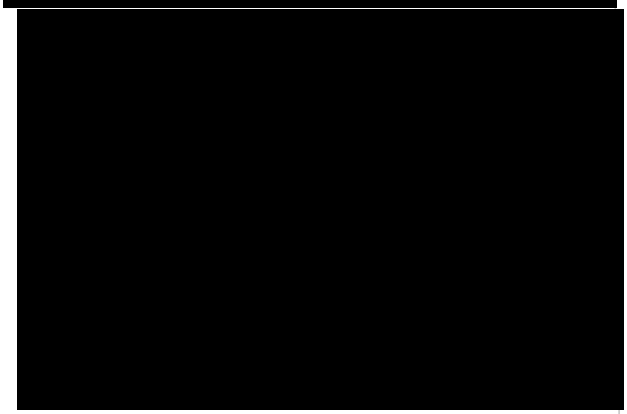


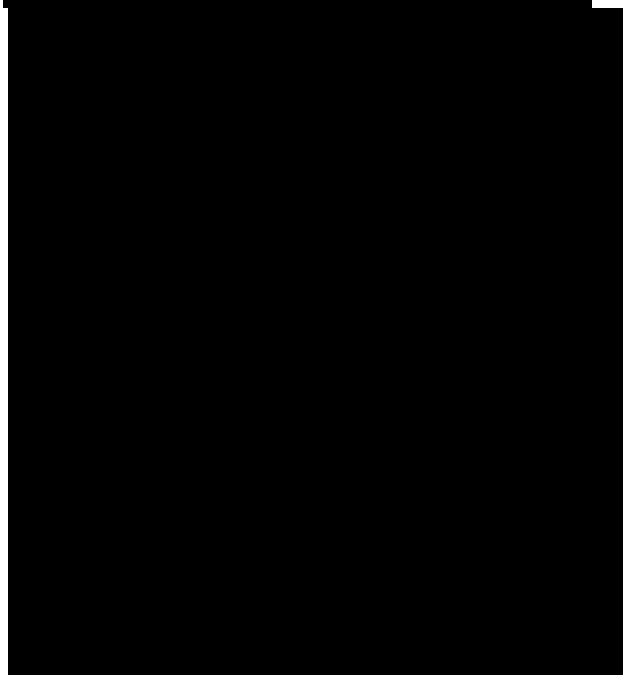


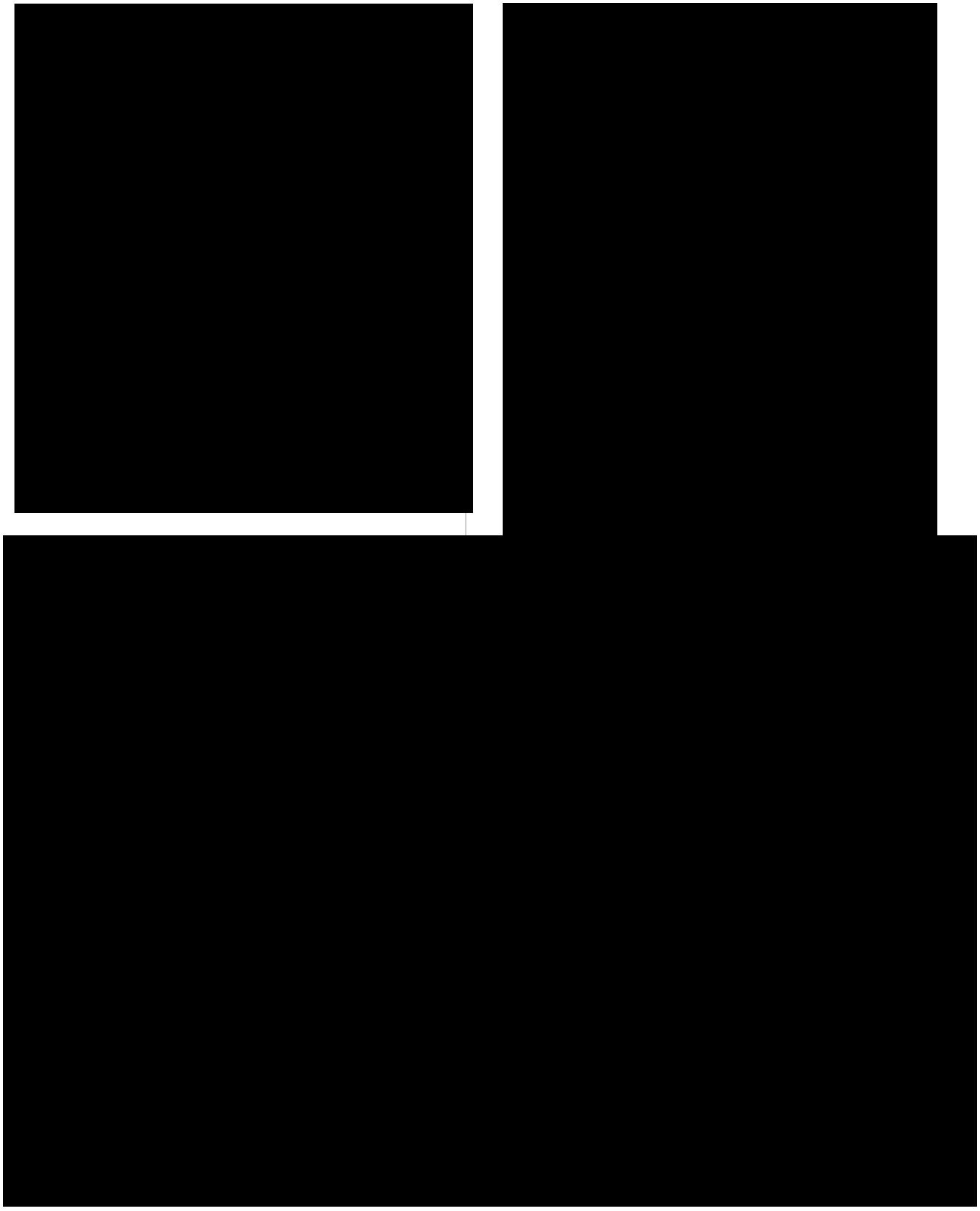


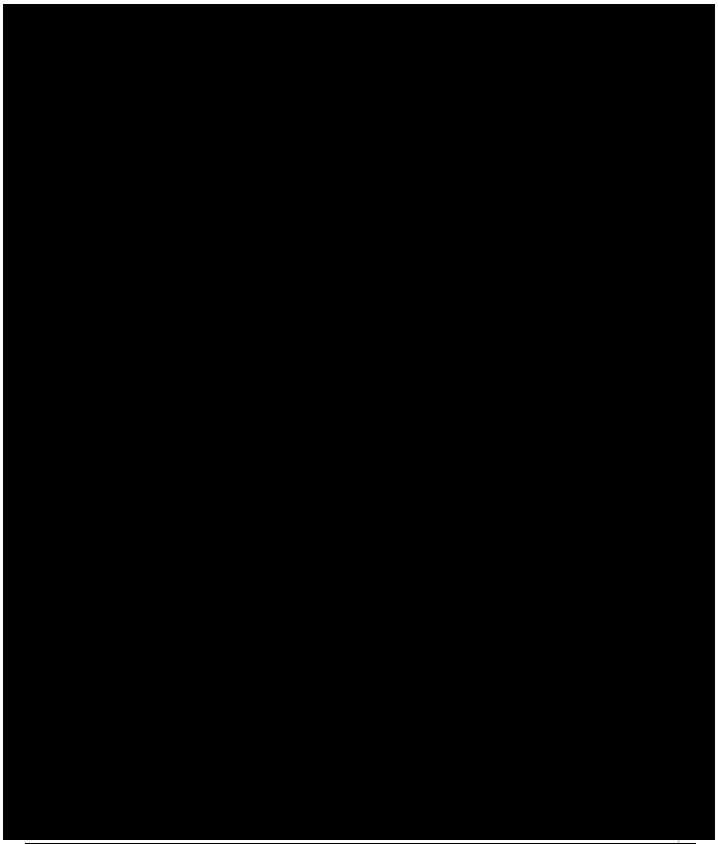


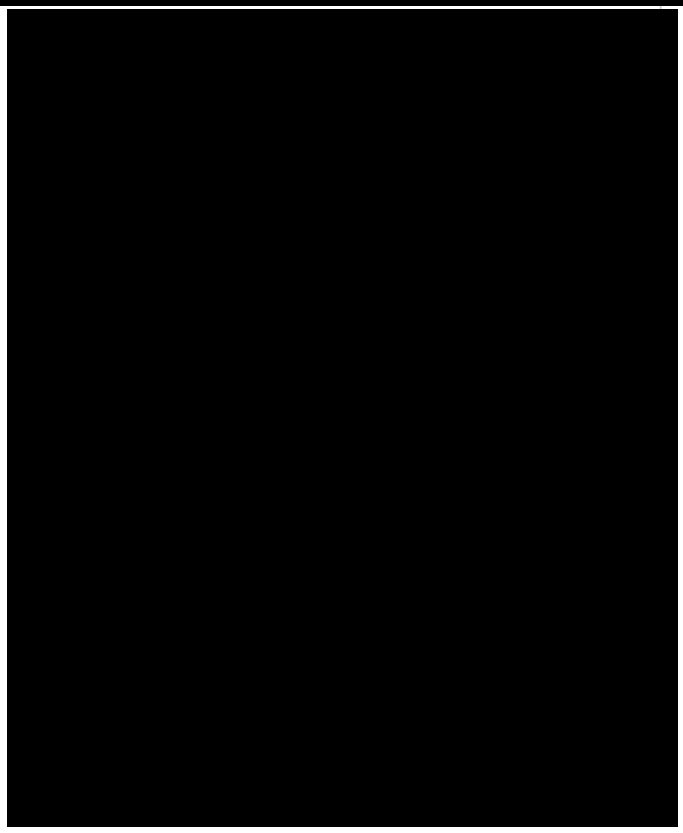


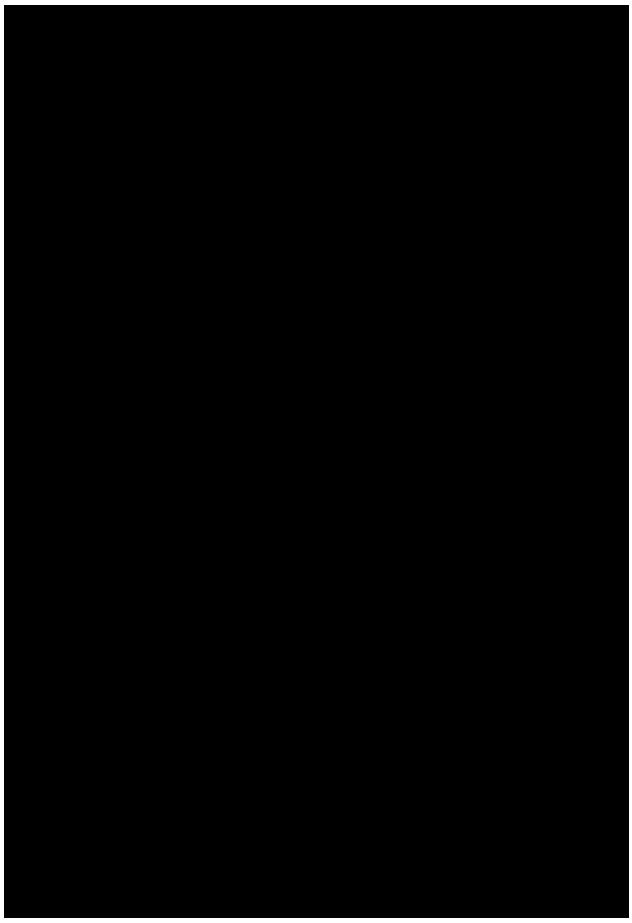


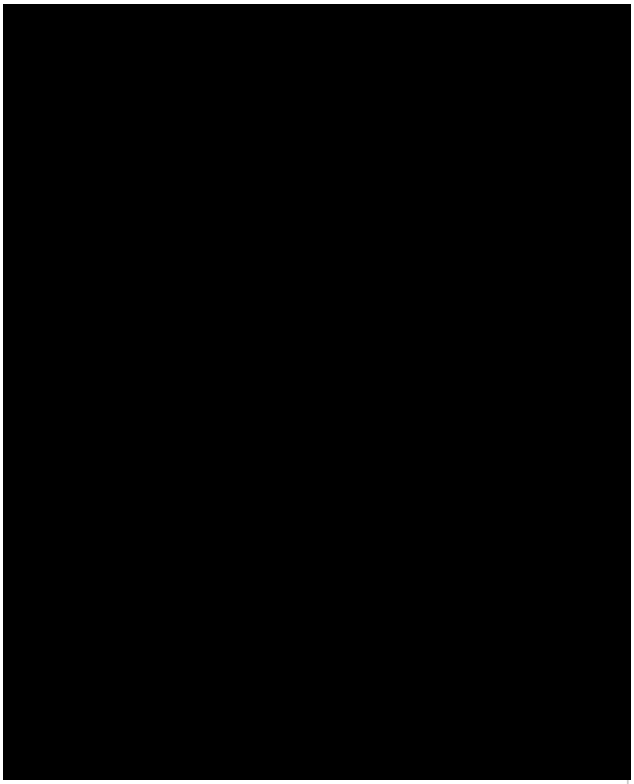


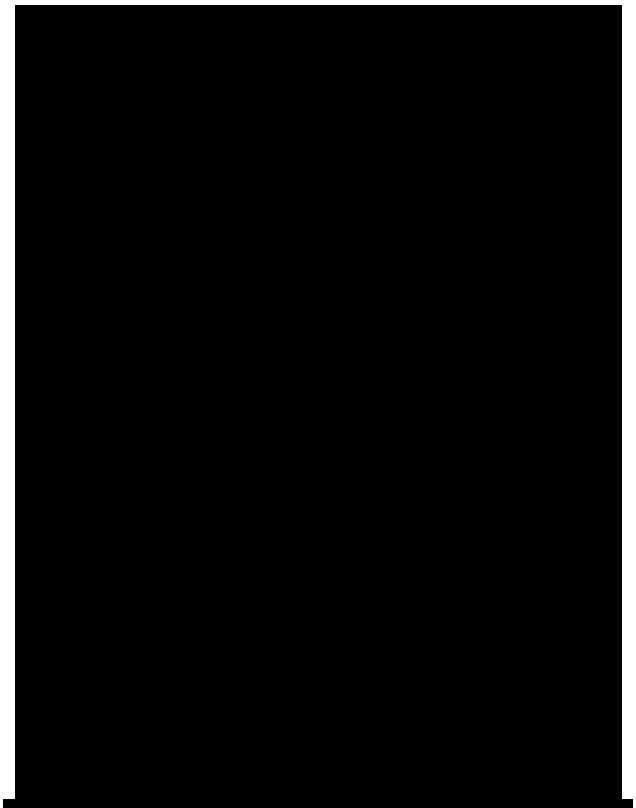


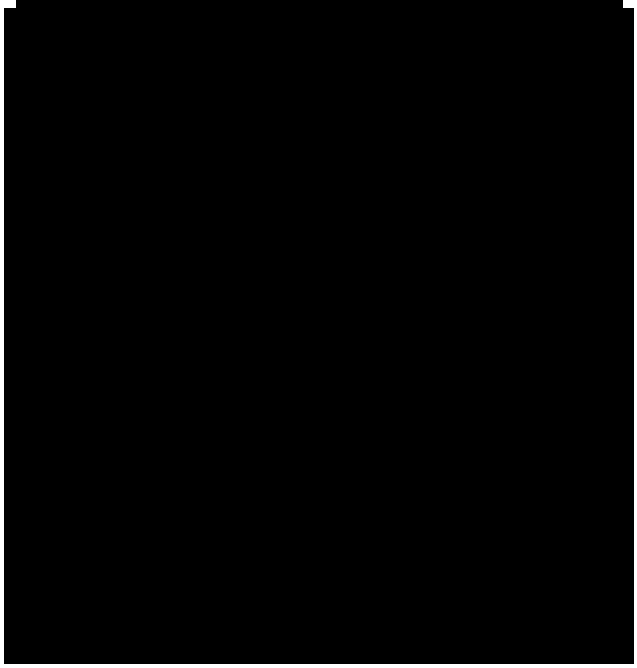


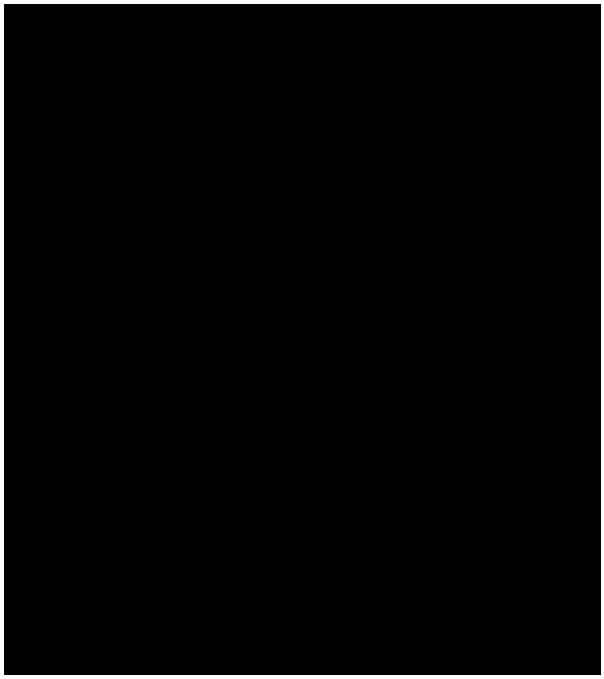


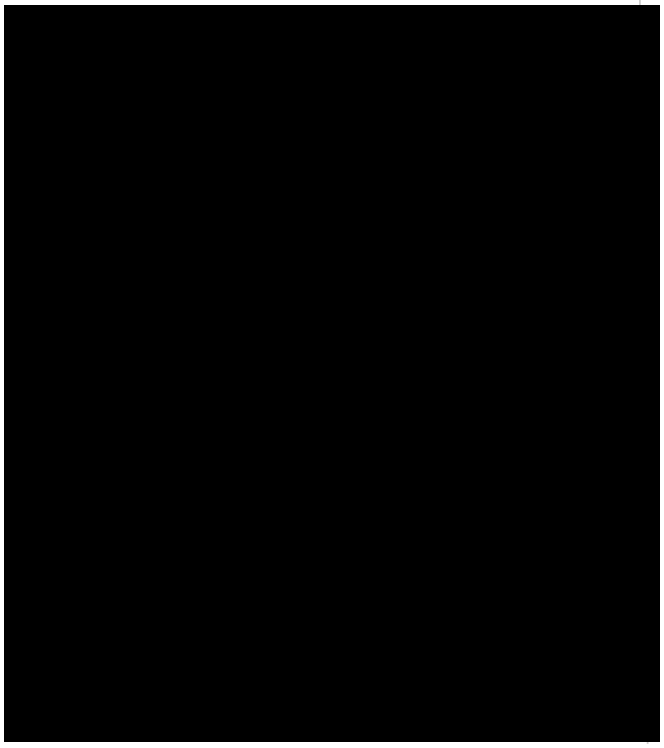


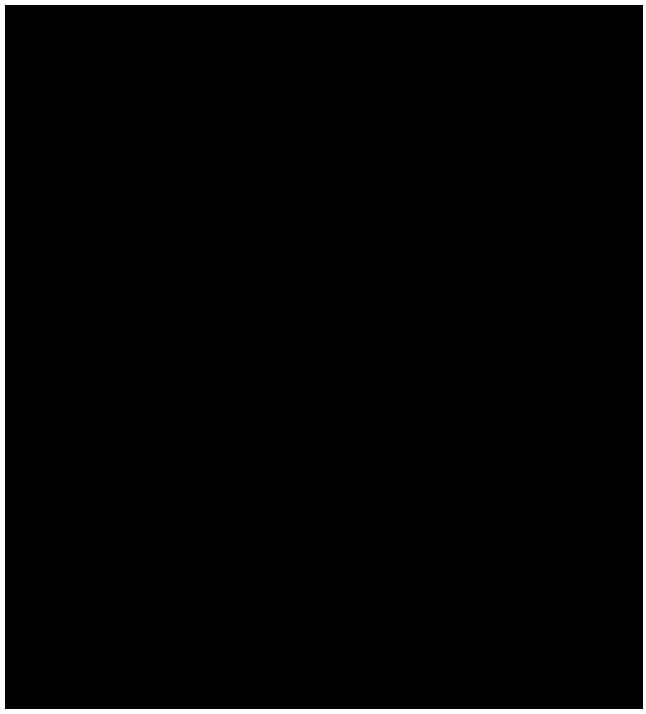


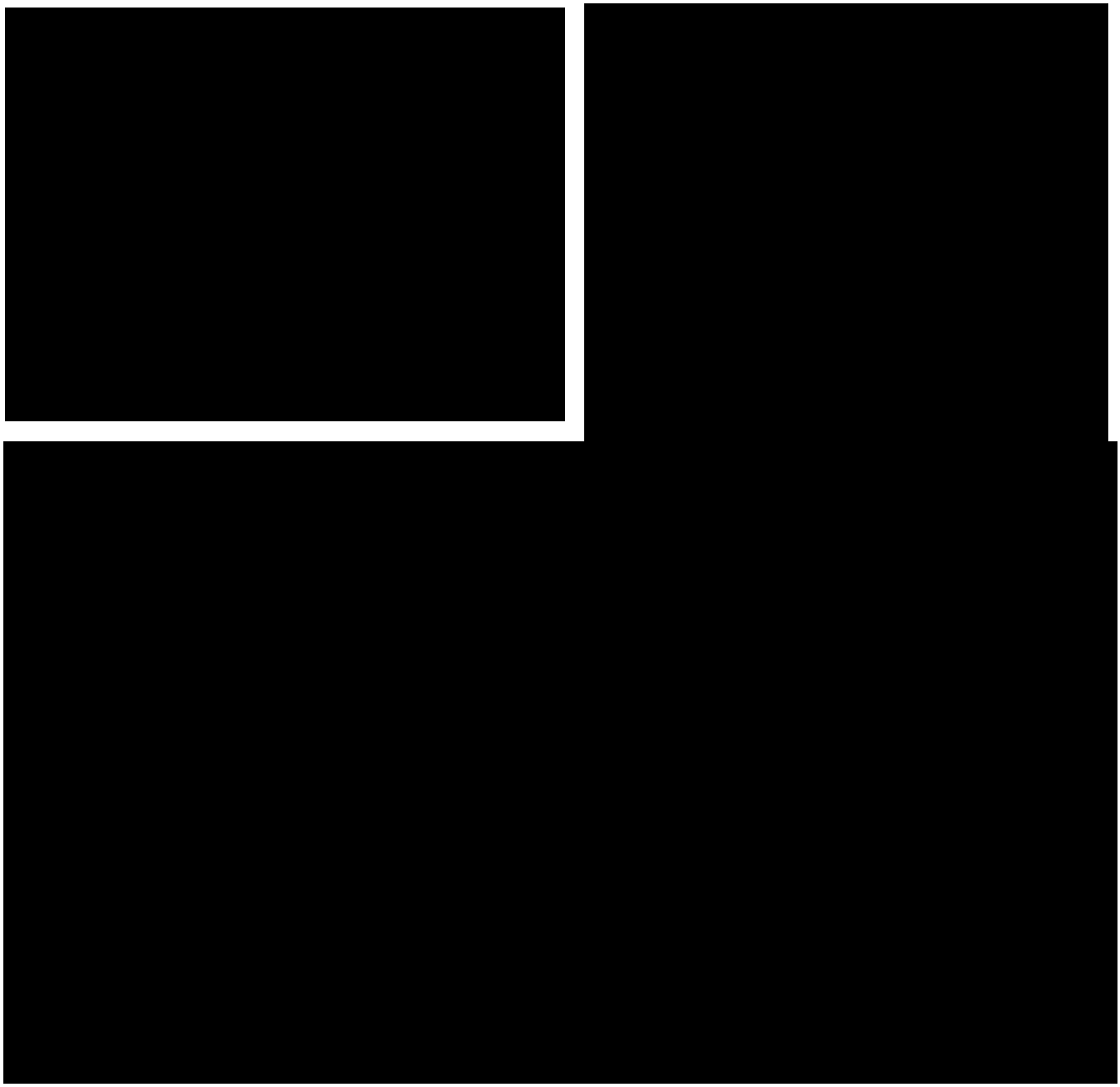












Q7(b) Contingency

SCHEDULE 12 – LOCAL PROTOCOLS

Section 1 - Overview

Background

1.1 In line with the requirements of paragraph 1.1A of section 4 of the Specification, the aim of this schedule is to outline general principles for interactions between the Supplier and Secure Establishments. Local Protocols have or will be made between the Supplier and each Secure Establishment set out in Schedule 7 (Secure Establishments).

1.2 For the avoidance of doubt, the responsibility for creating each Local Protocol sits firmly with the Supplier. The Supplier must create Local Protocols in collaboration with the Secure Establishment, and the Secure Establishment's approval of the Protocol(s) will be required in order for the Authority to agree these as final.

General principles

1.3 The independence of Advocates from those responsible for the care of Children and Young People in youth custody is a key principle of service and underpins safeguards that Advocates provide. The Supplier will, however, need to work in partnership with Secure Establishments to provide Children and Young People with effective and timely Advocacy Services support. Balancing this independence and partnership working may not always be easy, but a good balance will provide the best support and protection for Children and Young People.

1.4 Where possible the Service should assist Children and Young People to resolve issues at the lowest level, but, as it is paramount that the Service is led by young people, so there may be instances where, due to the young person's choice, issues may be pursued at a higher level.

1.5 Local safeguarding protocols between the Service and Secure Establishments will set out how Advocates will refer any safeguarding concerns to ensure appropriate safeguarding action is taken. The Protocols will also make clear where the confidentiality of Services to the young person is superseded by safeguarding or child protection duties.

1.6 Where a Child or Young Person requests to see an Advocate this should always be confidential, including following any incident, provided it is safe to do so.

1.7 Where the establishment does not believe it is safe to do so, the reasons for this should be discussed with the Advocate and with the Child or Young Person and recorded in writing.

Role of the Service Liaison Governor / Director

1.6 The Authority shall procure that each Secure Establishment shall ensure a sufficiently senior member of the management team - Governor/ Director, their Deputy, or a

nominated Head of Operating Function, or similar, with responsibility for the care of Children and Young People) is assigned the role of Service Liaison Governor/ Director to the Service. The assigned Governor/ Director should consistently attend Advocacy Review Meetings (ARMs) with the Supplier.

1.7 If the Service Liaison Governor/ Director is changed by the Secure Establishment the Supplier should be notified in writing. Any new or temporary Secure Establishment representative should be provided a handover of service documents e.g. protocols/ service specification and be in a position to progress and/ or feedback agreed action points from the previous meeting. This will ensure a consistent and proactive approach to taking a shared responsibility.

1.8 The Service Liaison Governor/ Director should read the monthly reports for the Secure Establishment (as per section 5 of the Specification) in advance of the scheduled monthly Advocacy Review Meetings and prepare areas of discussion/issues/themes to explore. Their role involves representing wider perspectives from the Secure Establishment to the Supplier, and equally sharing Service information and young people's views to their SMT colleagues to inform child-first effective, efficient and innovative practice. There will be an expectation that through representing the Secure Establishment, the Service Liaison Governor/ Director coordinates actions assigned to the Secure Establishment through monthly Advocacy Review Meetings, to progress issues and reach the best outcomes for Children and Young People.

1.9 The Service Liaison Governor/ Director will be central to coordinating should there be any instances of threats or perceived threats made to Supplier Staff onsite, the need for individual risk assessments, or important communications. In such circumstances, the liaison will take lead responsibility to ensure that Supplier Staff are safe whilst practicing onsite.

1.11 The Service Liaison Governor/ Director will be provided with emergency contact details for the Supplier, including out of hours, to be shared with all relevant departments at the relevant Premises.

1.12 The underlying principles of advocacy and of this Service include confidentiality and independence. The Service Liaison Governor/ Director will ensure that the Supplier is afforded the opportunity to practice accordingly, champion these vital requirements, and support them to overcome barriers to protect this important position and option for young people in their care.

Information and Communication

1.13 The Authority shall procure that Secure Establishments provide the Supplier with sufficient information to carry out their duties at each Premises. This includes informing Advocates of new arrivals, informing them when required of where and when they can speak to a young person and other areas as detailed further in the following sections.

1.14 Secure Establishments and the Supplier should agree locally how Children and Young People be provided with the necessary information, and how the Services can and will be publicised at each Secure Establishment to Children and Young People, their families, and to raise staff and visitor awareness of the Services. Local Protocols

should also agree arrangements for use by the Supplier of Secure Establishment facilities for interpretation services for Children and Young People.

1.15 The Supplier should minimise any impact on Children and Young Peoples' planned regime activities by trying, where possible and where the matter is non-urgent, to contact young people outside of core education hours and planned intervention / activity - i.e. before education, during lunch breaks or in the evenings and at weekends.

1.16 The Supplier will have in place local arrangements with each Secure Establishment to demonstrate effective internal stakeholder relationships, part of which are the Advocacy Review Meetings (ARMs) to be held between the Supplier and the Secure Establishment. The local arrangements will set out their responsibility for facilitating these meetings and providing minutes, which sits with the Supplier. These meetings will be used to monitor the effectiveness of the Service and discuss local issues which may arise. All parties are requested to provide consistent attendance at these meetings to allow for the development of constructive working relationships. Where urgent issues arise between meetings, Secure Establishments and the Supplier should make all reasonable efforts to resolve issues locally.

1.17 The Local Protocols will be reviewed in collaboration with the Secure Establishments as required, and updated throughout the contract Term as required by the Supplier.

1.18 The Supplier will provide copies of the Local Protocols to the Authority whenever a significant change is agreed with the Secure Establishment, or as reasonably requested.

Section 2 – Advocacy Service Arrangements

Accessing Secure Establishments

2.1 The Specification (Schedule 1) includes provision for Supplier access to, office space within, and internet and/ or telephone access in each of the Secure Establishments listed in Schedule 7.

2.2 Local Protocols should outline expectations and requirements of the Supplier's Staff when working in a secure environment and any local arrangements needed regarding:

(a) Key/ radio training,
(b) Other training requirements for Supplier Staff operating at the Secure Establishment.

Notifications to the Supplier

2.3 The Authority has designed the Services to be easily available and accessible to Children and Young People in youth custody. So that the Supplier can operate the Services to the requirements contained in Schedule 1 and the timeframes/ targets agreed in Annex A (CDIs) of Schedule 10, Local Protocols must agree arrangements for the Supplier receiving timely notifications from Secure Establishment staff for each Child or Young Person:

(a) Newly arriving at a Secure Establishment.
(b) For whom any referral for Advocacy Services is made by Secure Establishment or other staff.
(c) For whom an urgent request is made by Secure Establishment or other staff:
    (i) Following any full search (at the Secure Establishment), or
    (ii) Where the Serious Injury and Warning Sign (SIWS) procedure is activated, following restraint.

2.4 In most cases, providing the Supplier with the Child or Young Person's name and location within the Secure Establishment will be sufficient for Advocates to respond or make contact.

2.5 In return, Local Protocols must agree arrangements for the Supplier to:
(a) Refer any safeguarding or security concerns to the Secure Establishment as soon as is reasonably practicable and before the Supplier leaves the establishment.

(b) Pass any allegations made to the Supplier against Secure Establishment staff members to the Secure Establishment as a safeguarding referral.

Notification of Arrival

2.6 The Supplier will receive notification from the Secure Establishment of a new Child or Young Person's arrival to the Secure Establishment as soon as is reasonably possible. The process for such notification will be agreed between the Supplier and Secure Establishment and written into each Local Protocol.

2.7 The notification arrangement at paragraph 2.6 will provide information such as the Child or Young Person's name(s), their YOI/ STC number, date of arrival and location within the Secure Establishment.

2.8 The Supplier and Secure Establishment will agree, via Local Protocols how the Secure Establishment will notify the Supplier in such scenarios as when a Child or Young Person is:
(a) Admitted directly to health care (rather than an induction or normal residential unit).
(b) Residing on the Care and Separation Unit (CSU).
(c) Fast-tracked through the Secure Establishment induction procedure (usually where they are familiar with or have already recently undertaken this).
(d) Lodged at the Secure Establishment for a limited period.
(e) On a Restricted Status.

Induction

2.9 The Supplier will ensure Local Protocols agree arrangements for visiting each Child or Young Person during their induction to the Secure Establishment, and for providing each child and young person with a session during their induction on Children and Human Rights.

2.10 So that the Supplier shall conduct all induction sections for Children and Young People away from staff and peers, access to confidential space is to be provided by the Secure Establishment.

Unit Visits

2.11 The Supplier is required to undertake on a weekly basis the minimum number of Unit Visits at each Secure Establishment – in line with the requirements in section 1 and as specified in paragraph 2 of Schedule 7 (Secure Establishments). The frequency and timetabling of such activity will be agreed for and with each Secure Establishment.

2.12 The agreed schedule for Supplier Unit Visits at each Secure Establishment will be shared with staff and Children and Young People at that Secure Establishment in line with the requirements in section 1 of the Specification and with the Authority as part of the management information included in each Monthly Data Return.

2.13 The Supplier will also visit units where Young People may be located temporarily, such as specialist units, healthcare, care and separation, or intensive support units.

2.14 The Secure Establishment will provide the Supplier with all relevant policies and procedures regarding safety and security when visiting units/ wings. The Supplier shall ensure all such procedures are incorporated into the Local Protocols and agreed with each Secure Establishment.

Referrals for Advocacy Services, Support and Urgent Requests

2.15 The Supplier is required to contact each Child or Young Person in response to a referral or an urgent request for advocacy within the timeframes given in paragraph 4.5.3 of section 4 of the Specification.

2.16 Local Protocols should make clear for each Secure Establishment how Children and Young People will be supported to make referrals and urgent requests to the Supplier, as well as the arrangements for Secure Establishment and other staff in making a referral or urgent request on a Child or Young Person's behalf.

2.17 Such arrangements must allow for timely and easily accessible advocacy support to Children and Young People in response to staff concerns.

2.18 Secure Establishments should notify the Supplier as soon as is practically possible with any referral or urgent request, clearly identifying the child or young person(s) concerned (and their location within the Secure Establishment, where the Supplier does not already know this).

Support at Meetings

2.19 Where possible, Children and Young People should be able to request to access the support of Advocates for any meetings they are involved in. This includes remand or sentence planning meetings; LAC reviews; behaviour management, behaviour intervention or violence reduction plans; restraint debriefs; adjudications (YOIs only

which are governed by PSI 05/2018, which sets out the process including the ability to adjourn if an advocate is not available to attend where requested by a Child or Young Person to act as a Mackenzie Friend); mediations between Children and Young People and staff; Child or Young Person forums or consultations; and placement review procedures.

2.20 Local Protocols must include arrangements for the Secure Establishment notifying the Supplier as soon as practically possible for cases where the Child or Young Person indicates they would like an Advocate to be present at their meeting.

2.21 Secure Establishments should note the timeframes given in paragraph 4.5.3 of section 4 of the Specification that the Supplier is required to contact each Child or Young Person within – for a referral and for an urgent request – and ideally provide Advocates with at least this much notice of a request to attend with a Child or Young Person.

2.22 Where organising the meeting to allow the Advocate to attend would cause unreasonable delay or difficulty for other parties scheduled to attend (e.g. YOT, social services) Local Protocols should include arrangements for this being explained to the Child or Young Person and for the Advocate to be invited to the following meeting instead.

Complaints

2.23 Local Protocols should include arrangements for the Supplier to support Children and Young People where they wish to make a complaint – chiefly concerning the Secure Establishment operator or staff, but this can include arrangements for complaints about another service provider onsite.

2.24 (The Supplier is required to promote to Children and Young People the procedures for making complaints about the Services).

2.25 The Secure Establishment will ensure all appropriate instructions, orders and other relevant policies regarding complaints processes (including confidential access complaints) are shared with the Supplier. The Supplier shall ensure all Local Protocols devised comply with these pre-existing processes and standards.

2.26 Representation of informal complaints should be Child or Young Person-led, and may include the Advocate representing Children and Young Peoples' complaints directly to external agencies if the Child or Young Person requests this action.

2.27 Local Protocols will support Children and Young Peoples' issues being resolved informally but, where the issue cannot be resolved at the informal level and/ or the Child or Young Person wishes to pursue a formal complaint, Local Protocols will reflect that the Advocate should support the Child or Young Person to navigate the complaints systems and the available formal procedures. All agencies have complaints procedures and the Child or Young Person should be helped to find the appropriate route by which to complain, if that is their expressed wish.

2.28 Where the Child or Young Person requests assistance in writing out a complaint, this must be in their own words and not those of the Advocate. Local Protocols will make

clear that the response to the complaint be directed to the Child or Young Person, not the Advocate.

Incidents

2.29 The Local Protocol should set out arrangements for alerting onsite Advocates of incidents that risk the safety or security of staff or the Services.

2.30 This must include in the event of a serious incident within the Secure Establishment the agreed procedure and responsibilities for communicating relevant information and any changes in risk assessments in place between the Supplier and the Secure Establishment. Emergency contact details and clear lines of communication are to be provided in the Local Protocols. The Supplier will take the lead from the Secure Establishment in terms of risk and changes in practice and notify the Authority of any impact on Services.

2.31 The Local Protocol will also agree (ad hoc) arrangements for where the Secure Establishment notifies the Supplier of an incident so that they can provide and offer support to Children and Young People.

Section 3 – Optional Service Arrangements

3.1 Where the Authority may activate Optional Services as described by Section 6 of the Specification, Local Protocols will need adding to/ amending so that these also agree with Secure Establishments arrangements in the following areas:

(a) Schedule 1 and the timeframes/ targets agreed in Annex A (CDIs) of Schedule 10, Local Protocols must agree arrangements for the Supplier receiving timely notifications from Secure Establishment staff for each Child or Young Person:

(b) Notification to the Supplier of each Child or Young Person's (within scope) release or transition (to adult custody) date from the Secure Establishment (at least 15 weeks before release/ transition).

3.2 The Authority will work with the Supplier to agree the full scope of addition/ amendment required to Local Protocols as part of activating Optional Services, using the information provide within the Payment Mechanism (Schedule 2) and the Change Control mechanism (Schedule 3) in this Contract.

Annex A – Agreed Local Protocols

SCHEDULE 13 – MOBILISATION PLAN

1 This Schedule:

1.1 defines the process for the preparation and implementation of the Outline Mobilisation Plan and Detailed Mobilisation Plan; and

1.2 identifies the Milestones (and associated Deliverables) including the Milestones which trigger payment to the Supplier of the applicable Milestone Payments following confirmation by the Authority that the Milestone has been achieved (to the Authority's reasonable satisfaction).

2 OUTLINE MOBILISATION PLAN

2.1 The Outline Mobilisation Plan is set out in Annex 1.

2.2 All changes to the Outline Mobilisation Plan shall be subject to the Change control procedure at clause F4 provided that the Supplier shall not attempt to postpone any of the Milestones using the Change control procedure or otherwise.

3 APPROVAL OF THE DETAILED MOBILISATION PLAN

3.1 The Supplier shall submit a draft of the Detailed Mobilisation Plan to the Authority for approval within twenty (20) Working Days of the Commencement Date.

3.2 The Supplier shall ensure that the draft Detailed Mobilisation Plan includes details of activities that will be undertaken during mobilisation that are specific (including in terms of the dates and resource attached to them) and should include as a minimum:

3.2.1 Milestones that apply to mobilisation, which should as a minimum reflect the Milestones set out in the Outline Mobilisation Plan:

3.2.2 how the Supplier will ensure it is ready to begin providing Services which address the requirements of the Specification and this Contract by the Services Commencement Date;

3.2.3 activities that will be undertaken in relation to TUPE and the working relationships associated with any exiting supplier(s);

3.2.4 delivery of an organisational structure, including all management structures, roles, responsibilities and relationships;

3.2.5 process and activities that will be undertaken in order to have appropriate risk assessments in place, and in time for the Services Commencement Date;

3.2.6 process for the collection and delivery of CDI and management information and sign-off;

3.2.7 stakeholder communications plan;

3.2.8 a list of all Staff that will be working at each Secure Establishment together with status of security clearance;

3.2.9 for Staff who have not obtained security clearance, a plan to apply for and manage security clearance in time for delivery of the activities described in the Mobilisation Plan.

3.2.10 the list of activities required to enable the efficient and effective transfer of relevant information from exiting suppliers;

3.2.11 the list of any Supplier Equipment with dates for delivery;

3.2.12 requirements in terms of adjustments to Secure Establishments, equipment, and facilities;

3.2.13 a full and detailed timetable of delivery of the Services;

3.2.14 proposals for use of IT equipment, in line with requirements detailed in the Schedules to this Contract;

3.2.15 details of Sub-Contractors that will be used and relationship(s) with third parties;

3.2.16 proposals for invoicing (see paragraph 3.2.1 above);

3.2.17 delivery of equality and diversity statements;

3.2.18 delivery of an agreed Business Continuity Plan in accordance with Schedule 11.

3.3 Following receipt of the draft Detailed Mobilisation Plan from the Supplier, the Authority shall:

3.3.1 review and comment on the draft Detailed Mobilisation Plan as soon as reasonably practicable; and

3.3.2 notify the Supplier in writing that it approves or rejects the draft Detailed Mobilisation Plan no later than 20 Working Days after the date on which the draft Detailed Mobilisation Plan is first delivered to the Authority.

3.4 If the Authority rejects the draft Detailed Mobilisation Plan:

3.4.1 the Authority shall inform the Supplier in writing of its reasons for its rejection; and

3.4.2 the Supplier shall then revise the draft Detailed Mobilisation Plan (taking reasonable account of the Authority's comments) and shall re-submit a revised draft Detailed Mobilisation Plan to the Authority for the Authority's approval within 20 Working Days of the date of the Authority's notice of rejection. The provisions of paragraph 3.3 and this paragraph 3.4 shall apply again to any resubmitted draft Detailed Mobilisation Plan, provided that either Party may refer any disputed matters for resolution by the dispute resolution procedure set out in clause I1 at any time.

3.5 If the Authority approves the draft Detailed Mobilisation Plan, it shall replace the Outline Mobilisation Plan from the date of the Authority's notice of approval.

3.6 The Supplier's performance against the Mobilisation Plan shall be monitored at this Contract Review Meetings. In preparation for such meetings, the current Detailed Mobilisation Plan shall be provided by the Supplier to the Authority not less than 5 Working Days in advance of each Contract Review Meetings.

3.7 Save for any amendments which are of a type identified and notified by the Authority (at the Authority's discretion) to the Supplier in writing as not requiring approval, any material amendments to the Detailed Mobilisation Plan shall be subject to the Change control procedure at clause F4 provided that:

3.7.1 any amendments to elements of the Detailed Mobilisation Plan which are based on the contents of the Outline Mobilisation Plan shall be deemed to be material amendments; and

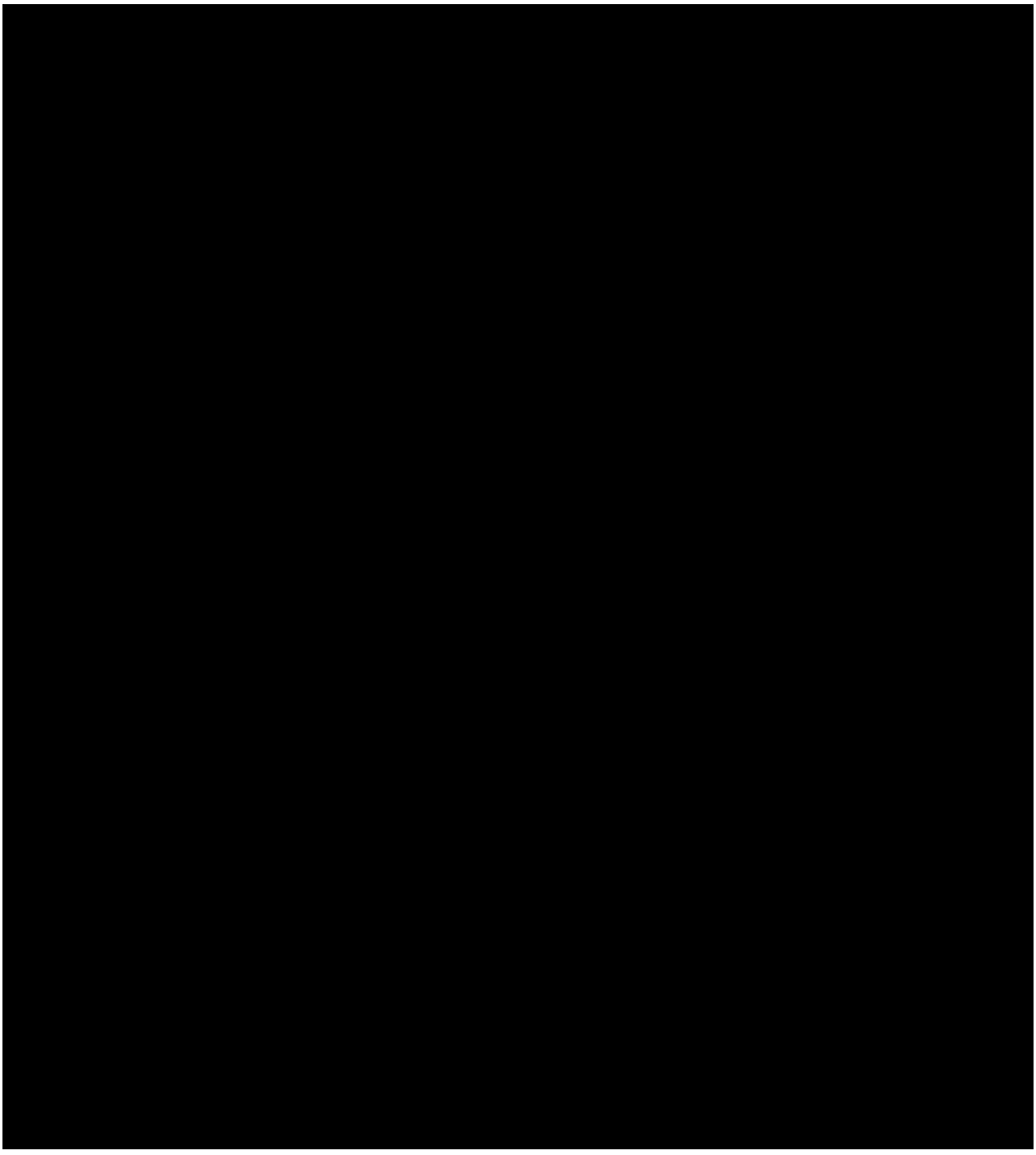
3.7.2 in no circumstances shall the Supplier be entitled to alter or request an alteration to any Milestone Date.

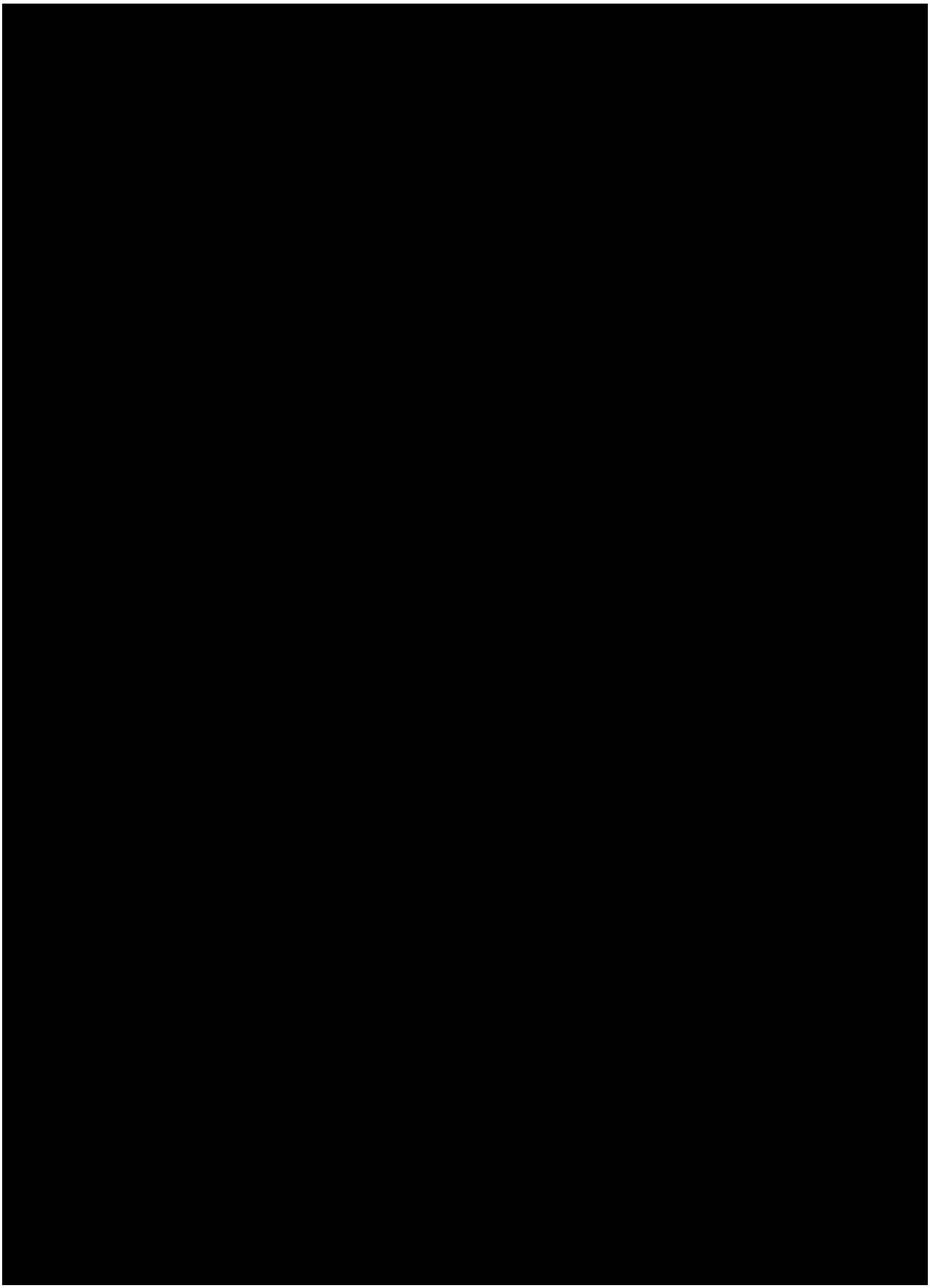
3.8 Any proposed amendments to the Detailed Mobilisation Plan shall not come into force until they have been approved in writing by the Authority.

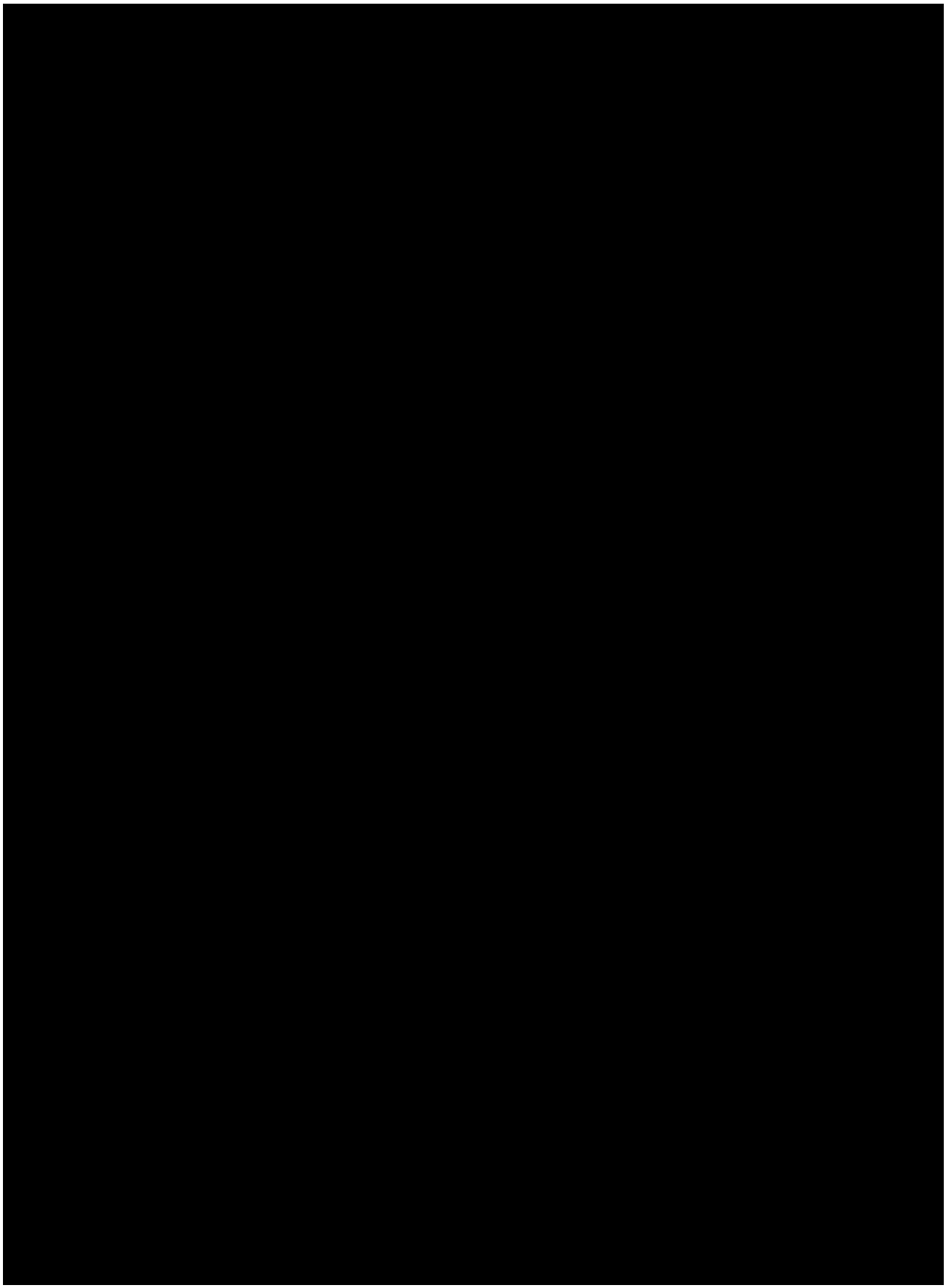
4 GOVERNMENT REVIEWS

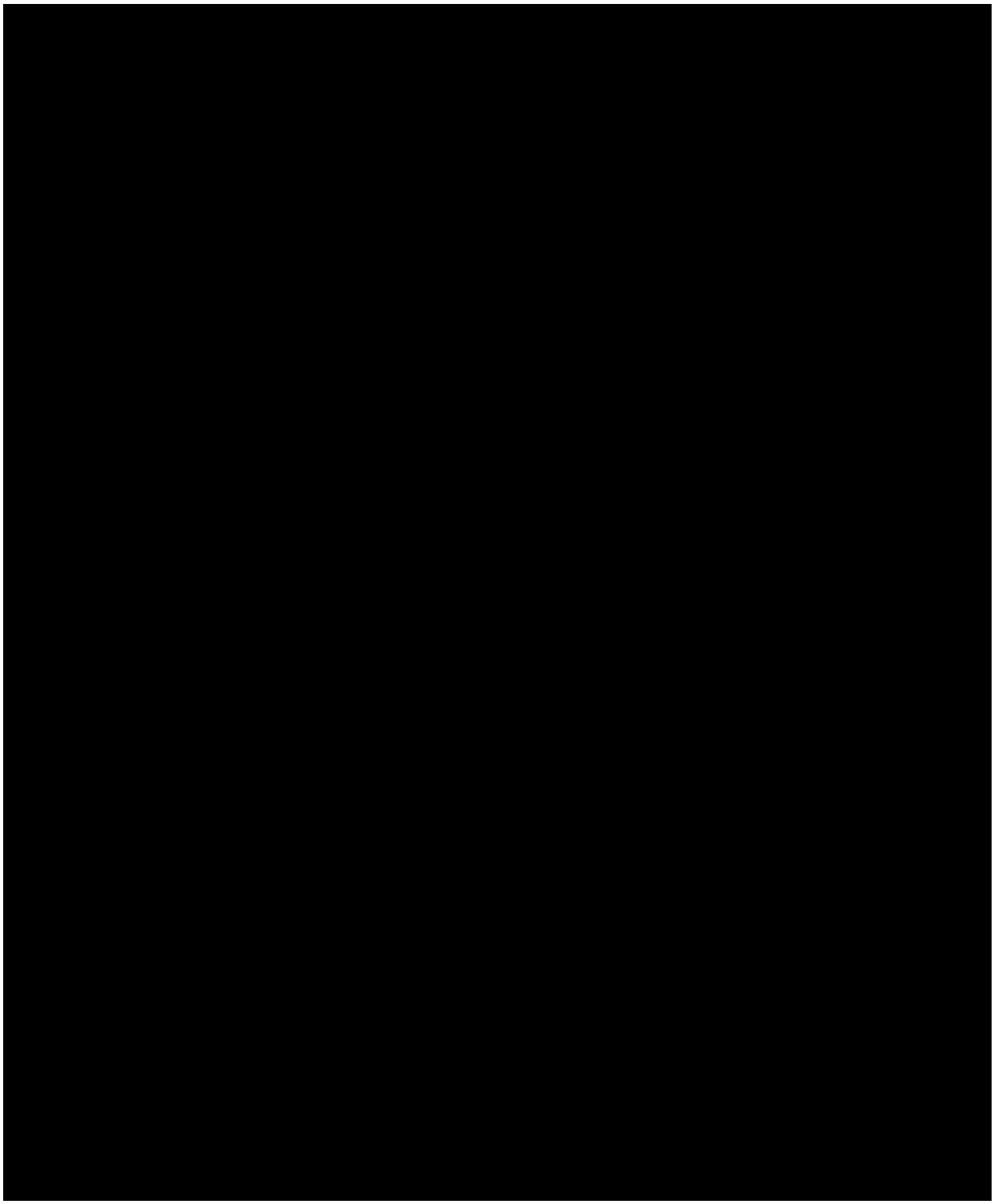
4.1 The Supplier acknowledges that the Services may be subject to Government review at key stages of the project. The Supplier shall cooperate with any bodies undertaking such review and shall allow for such reasonable assistance as may be required for this purpose within the Charges.

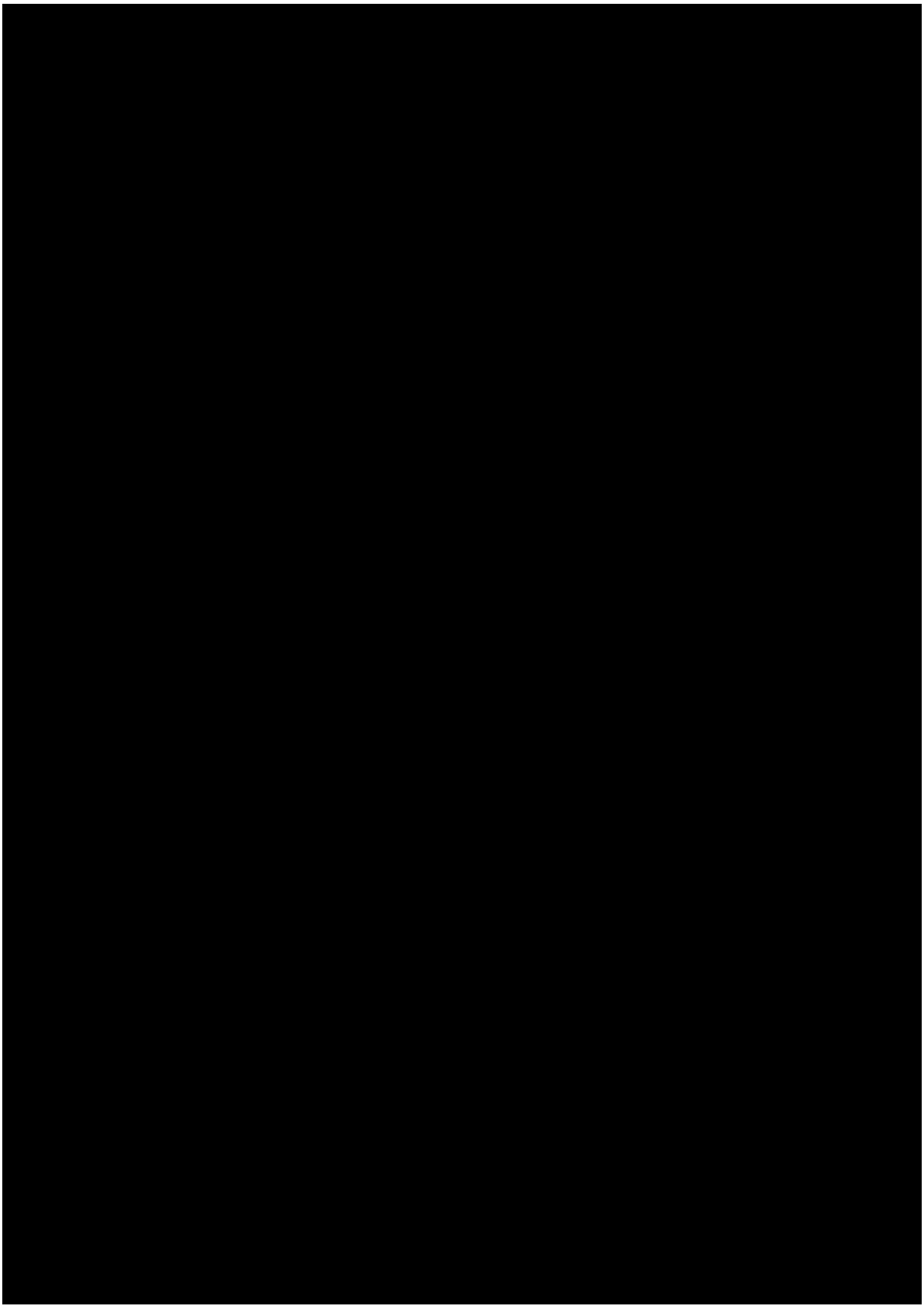
ANNEX 1: OUTLINE MOBILISATION PLAN

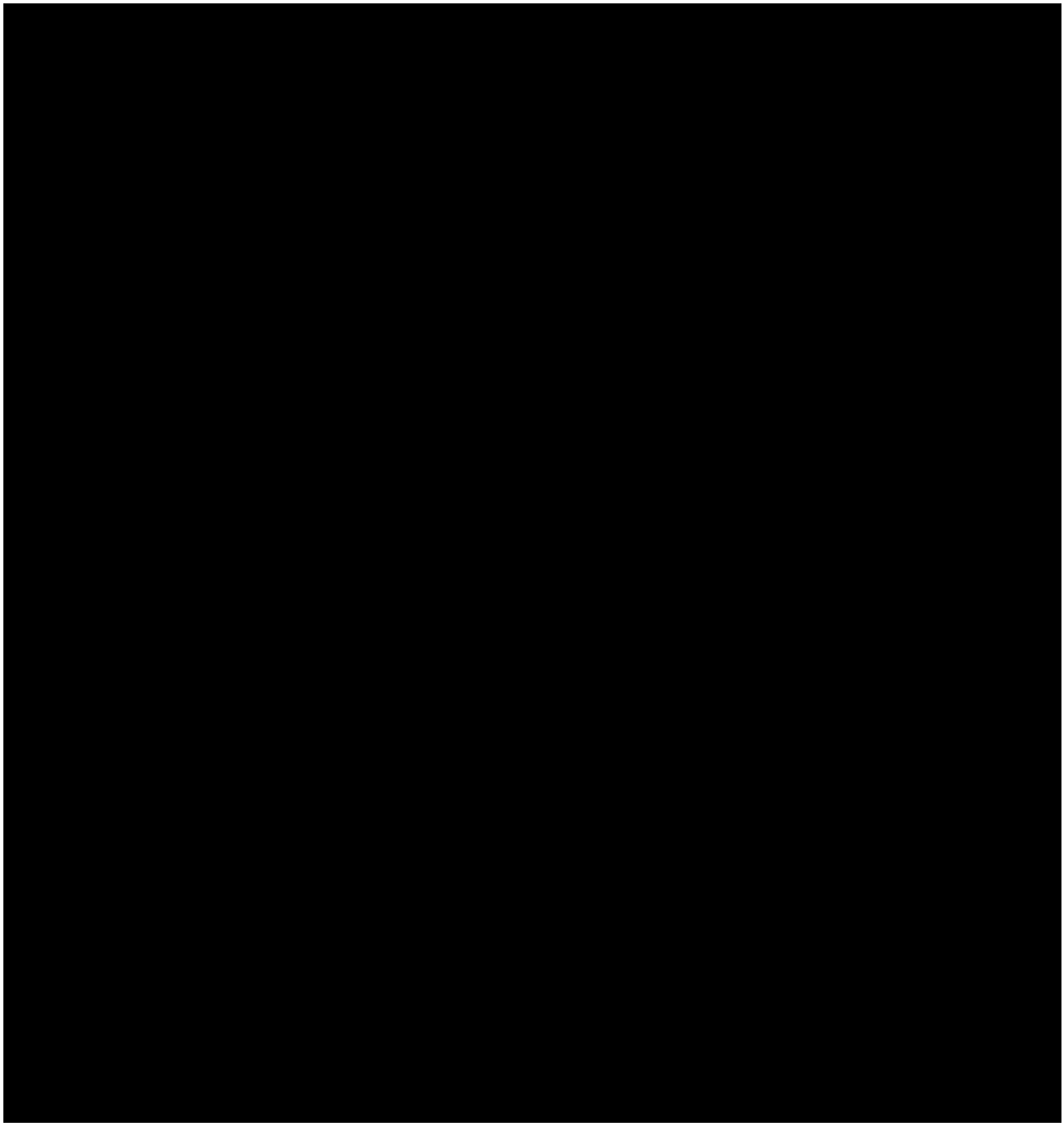


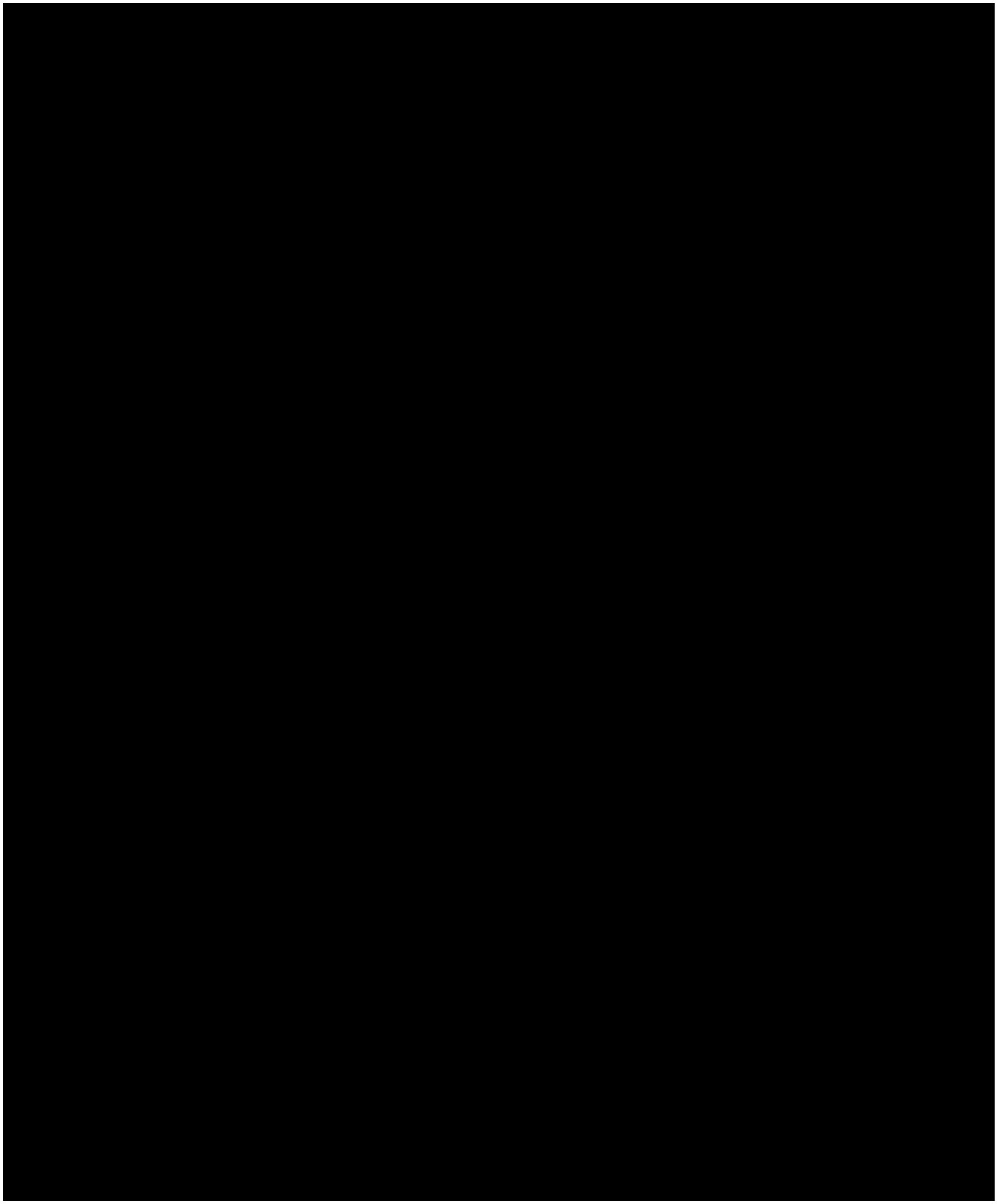


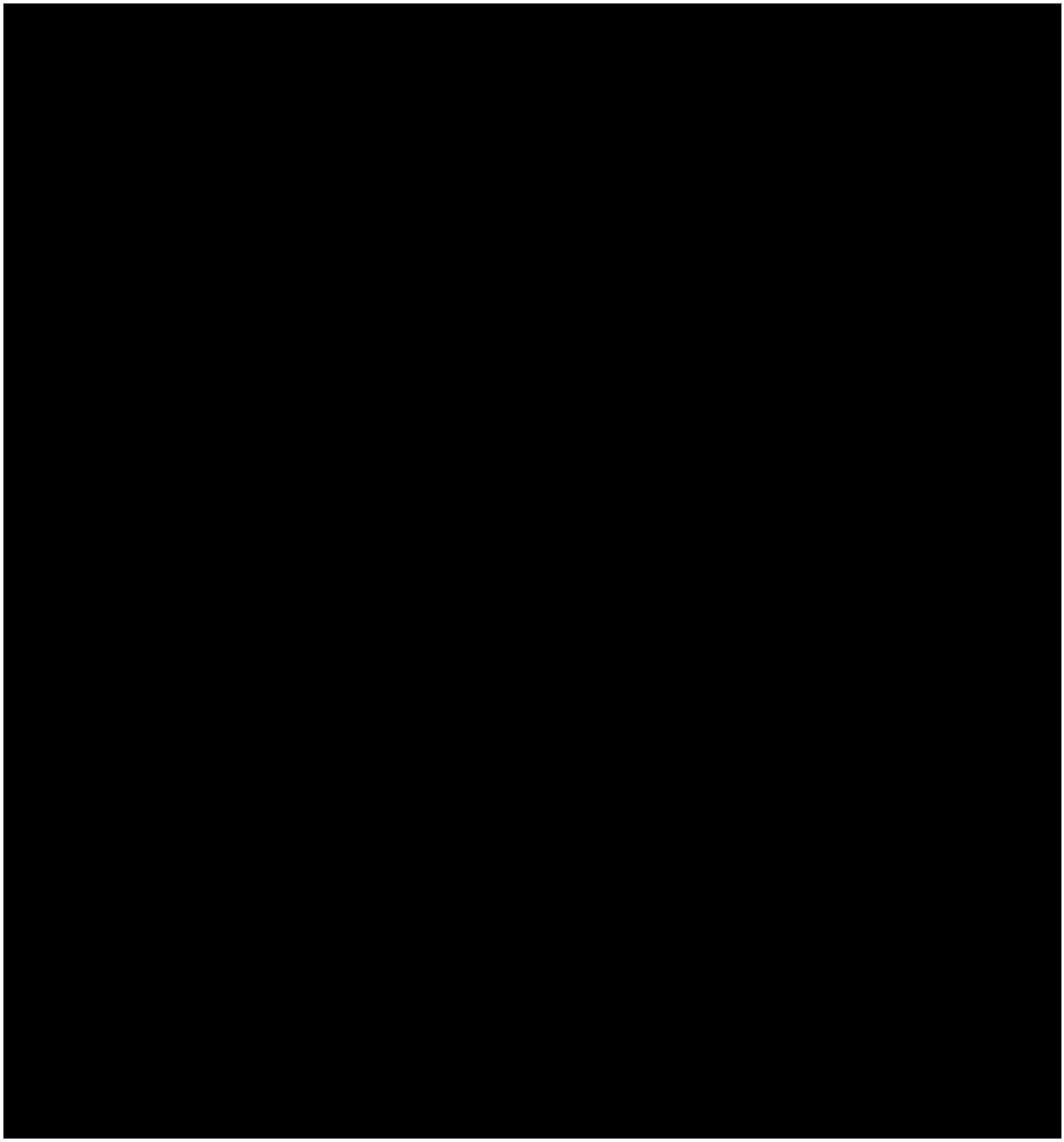


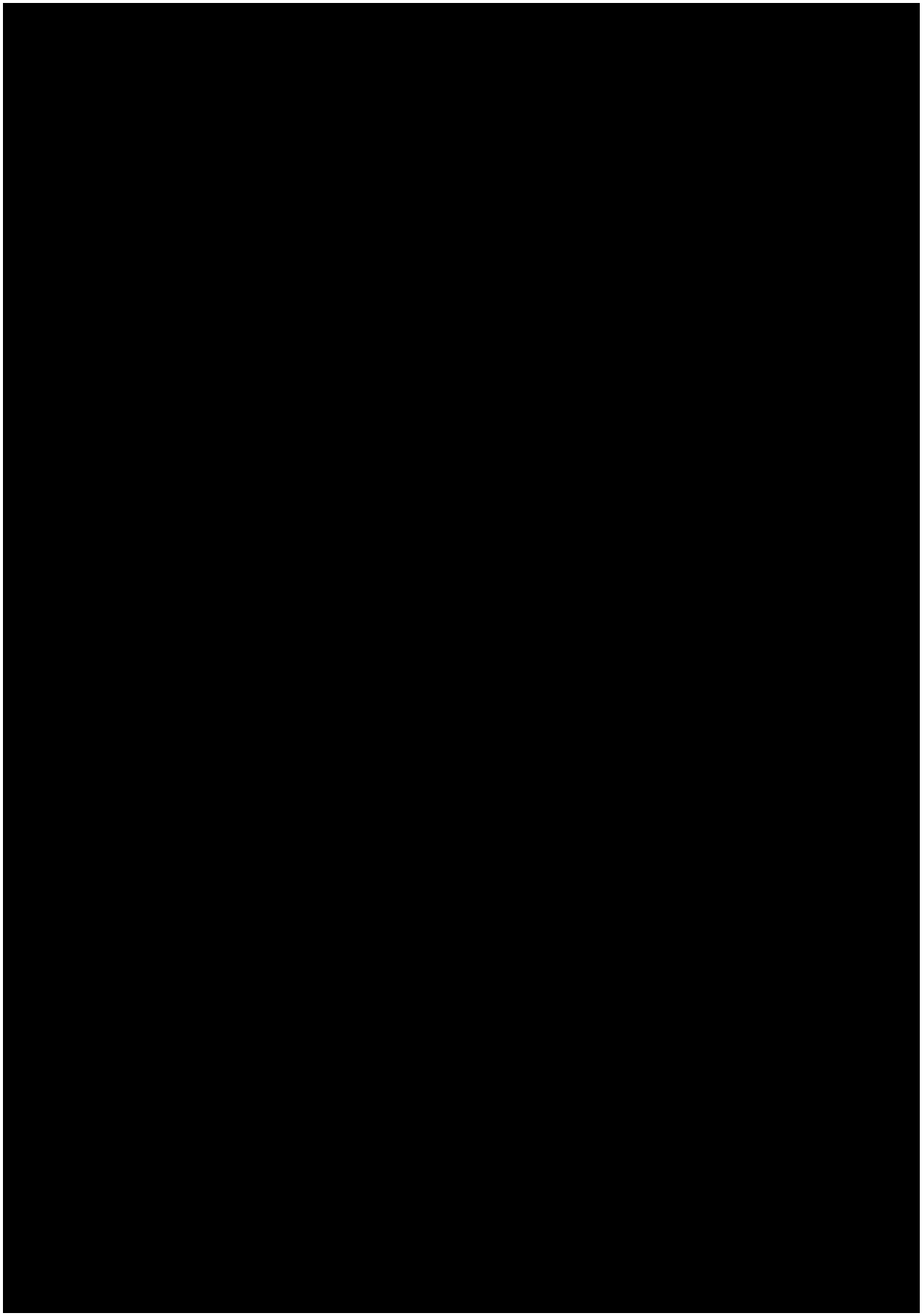


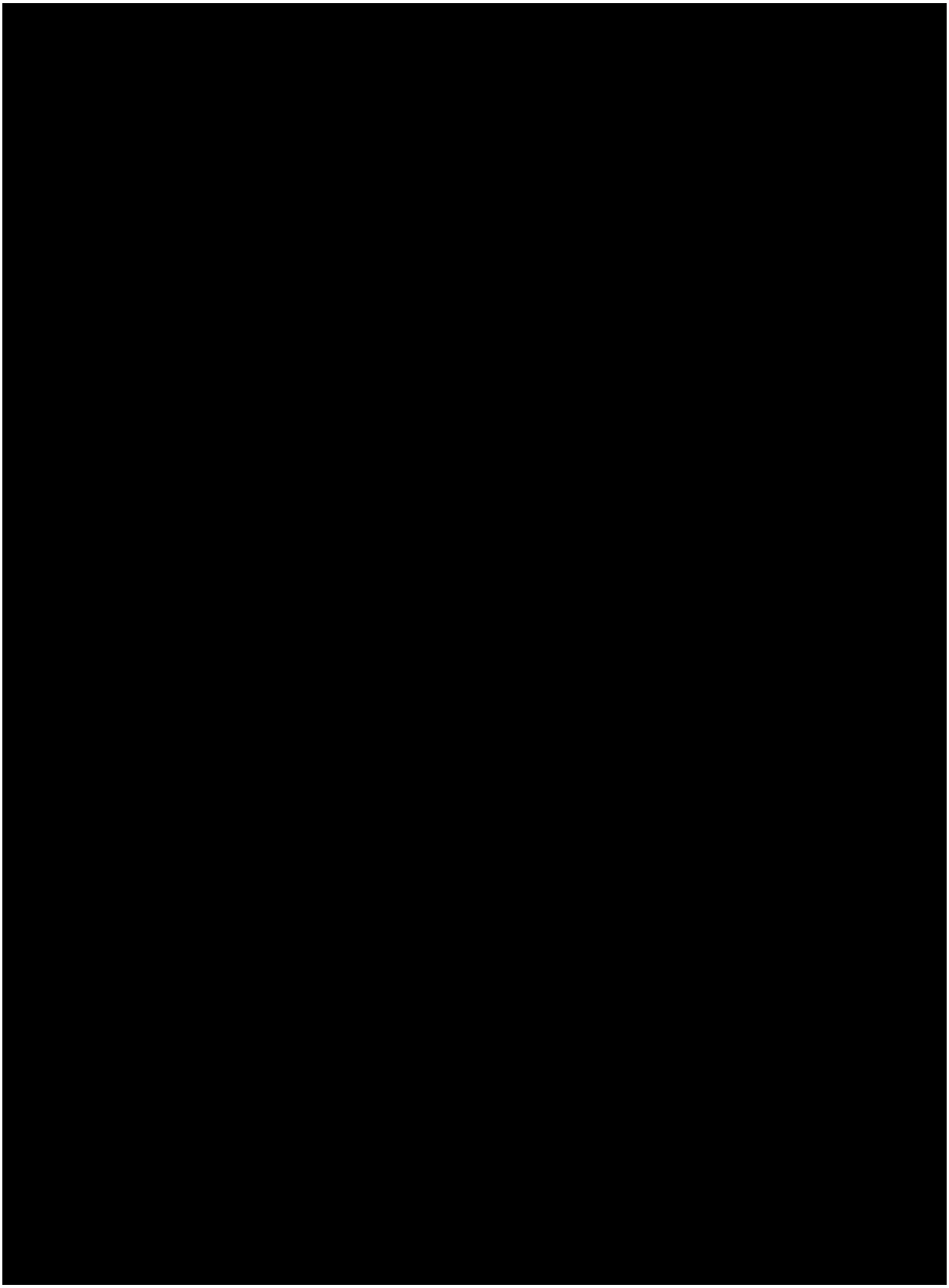


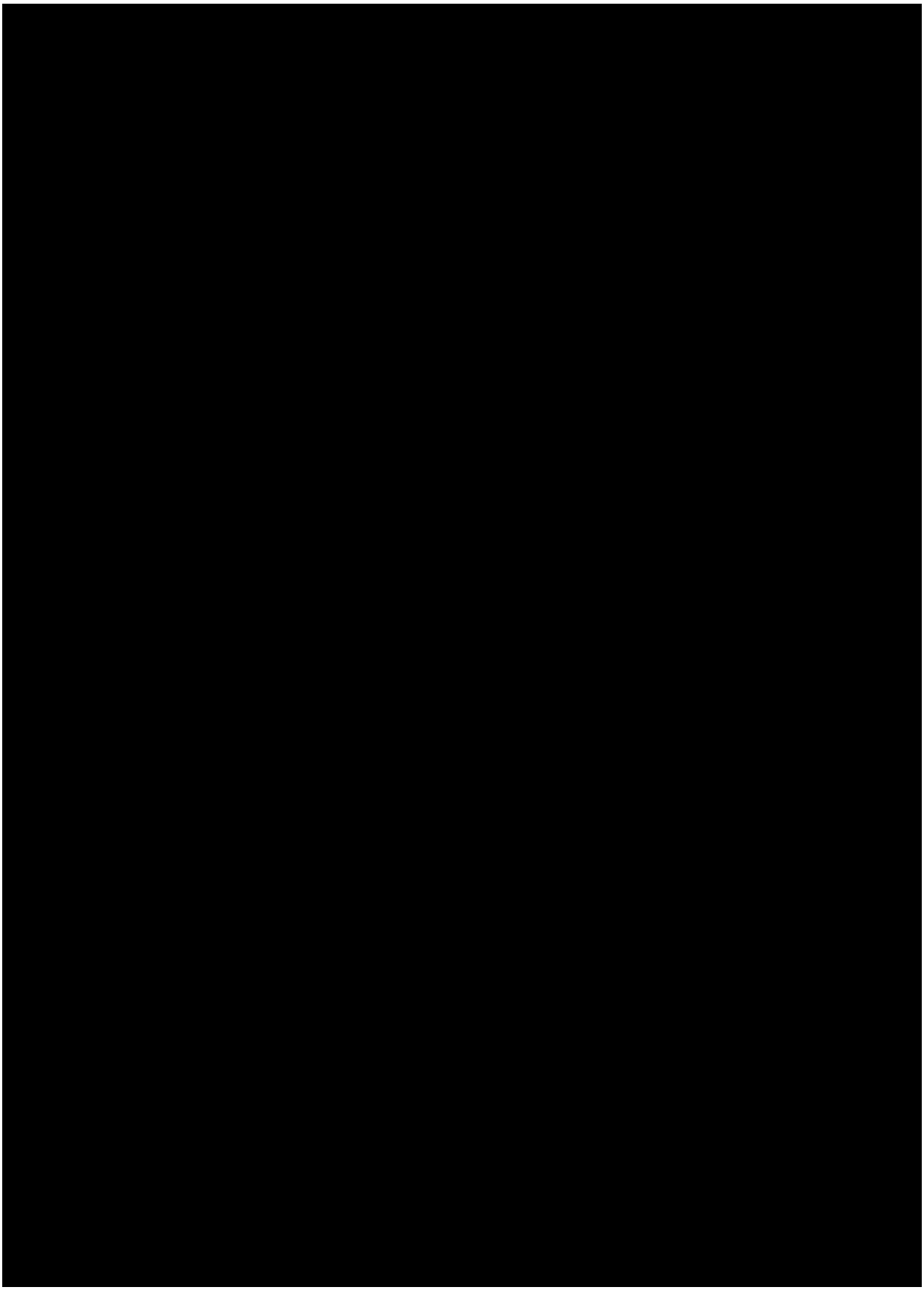


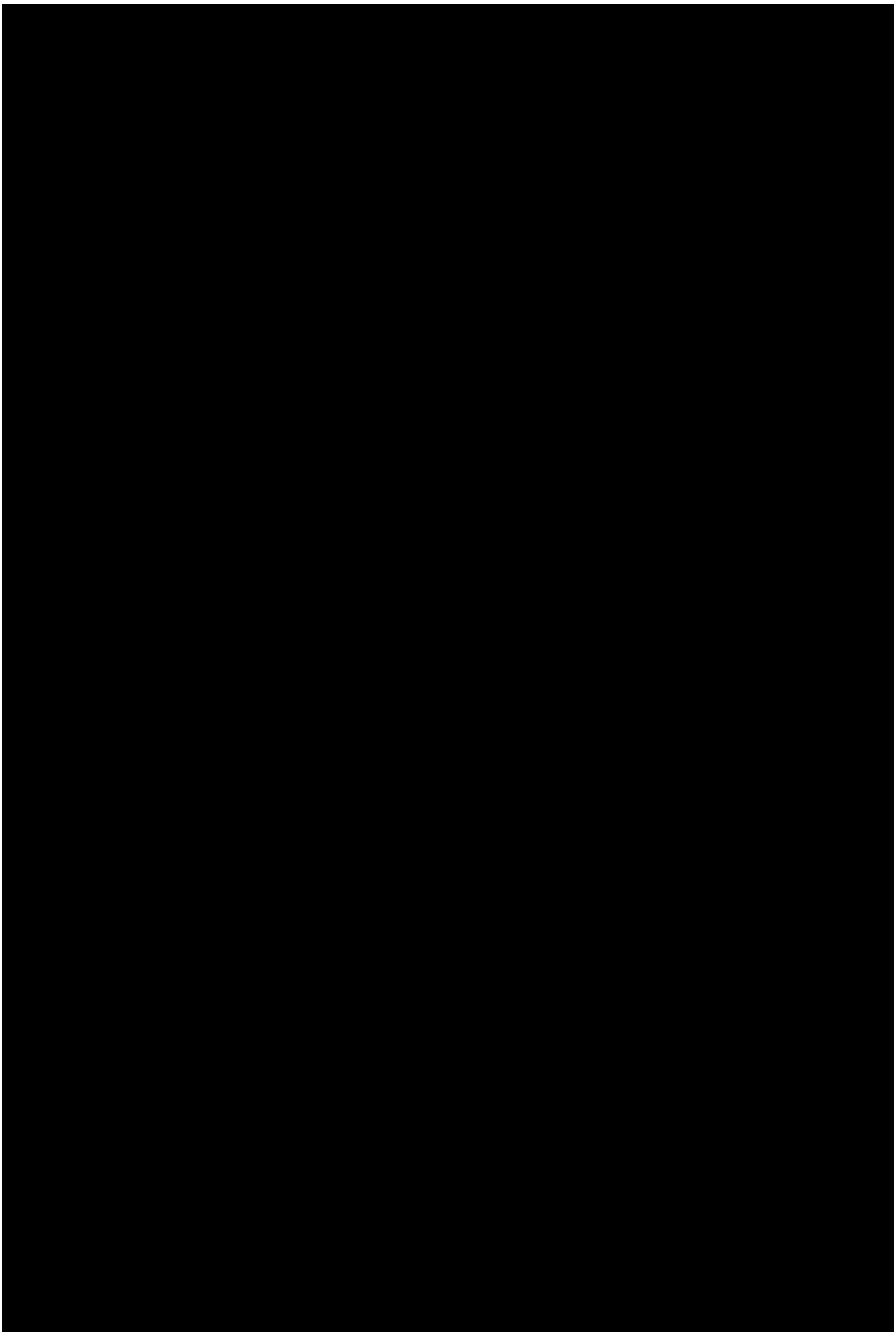


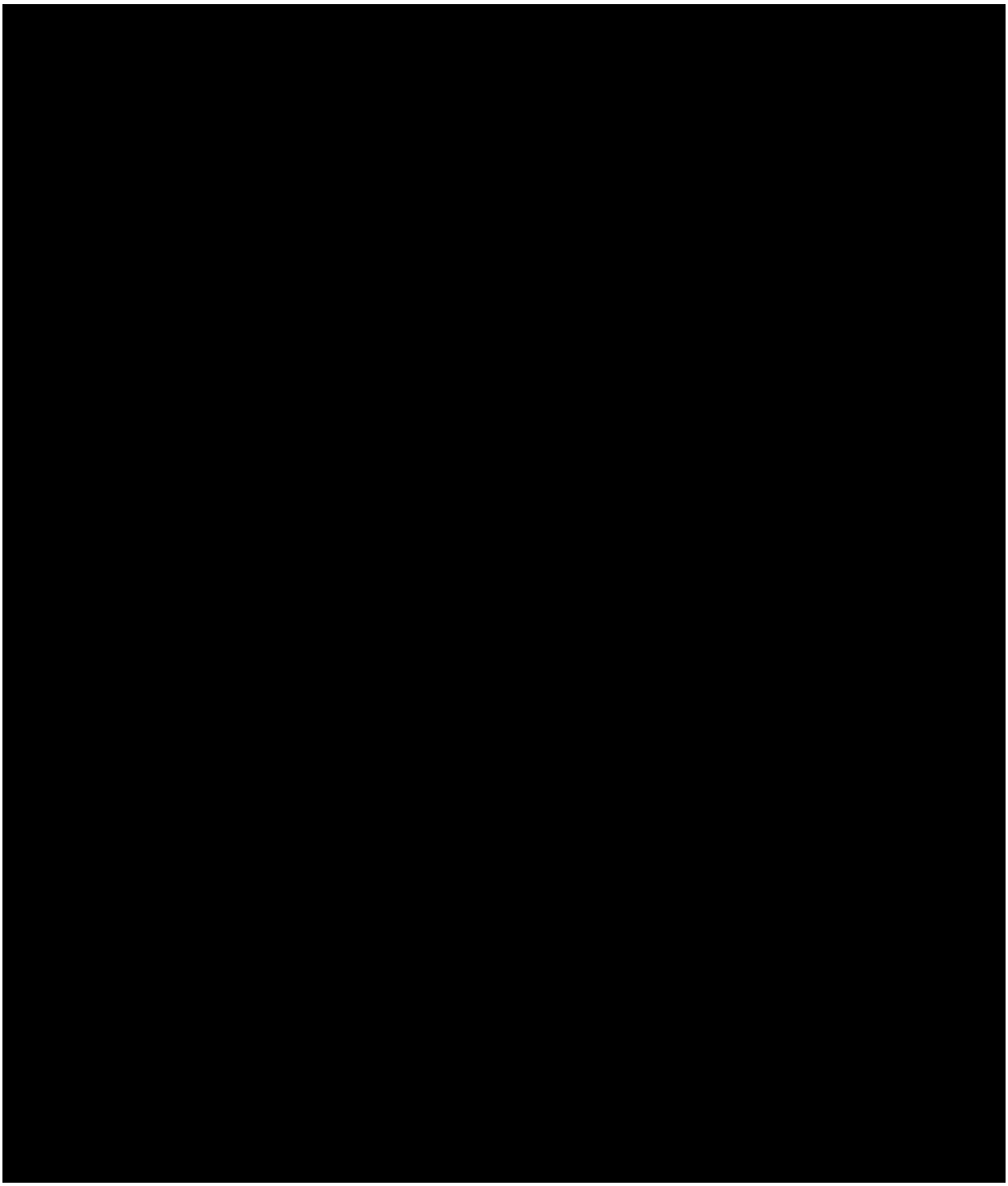


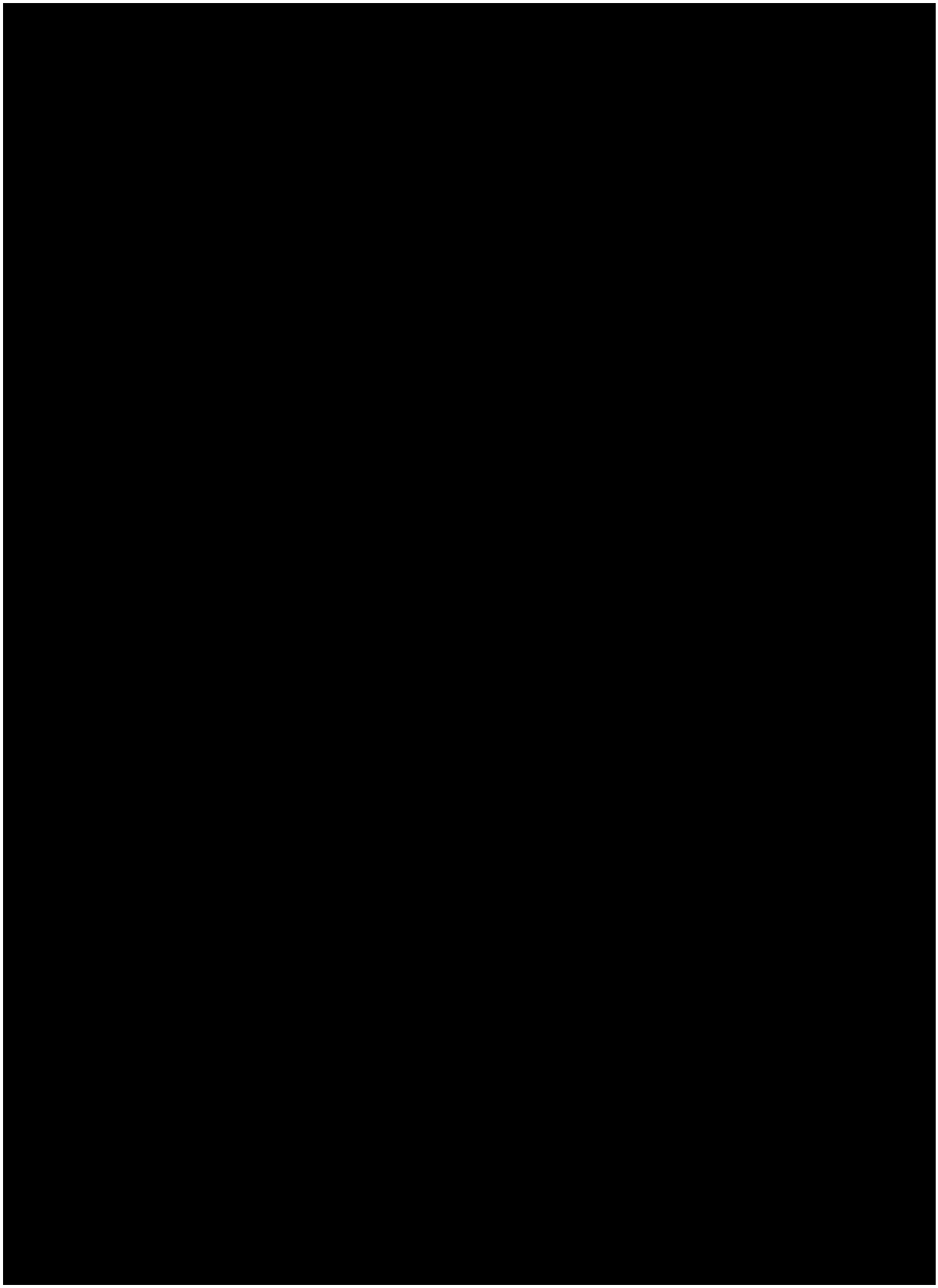


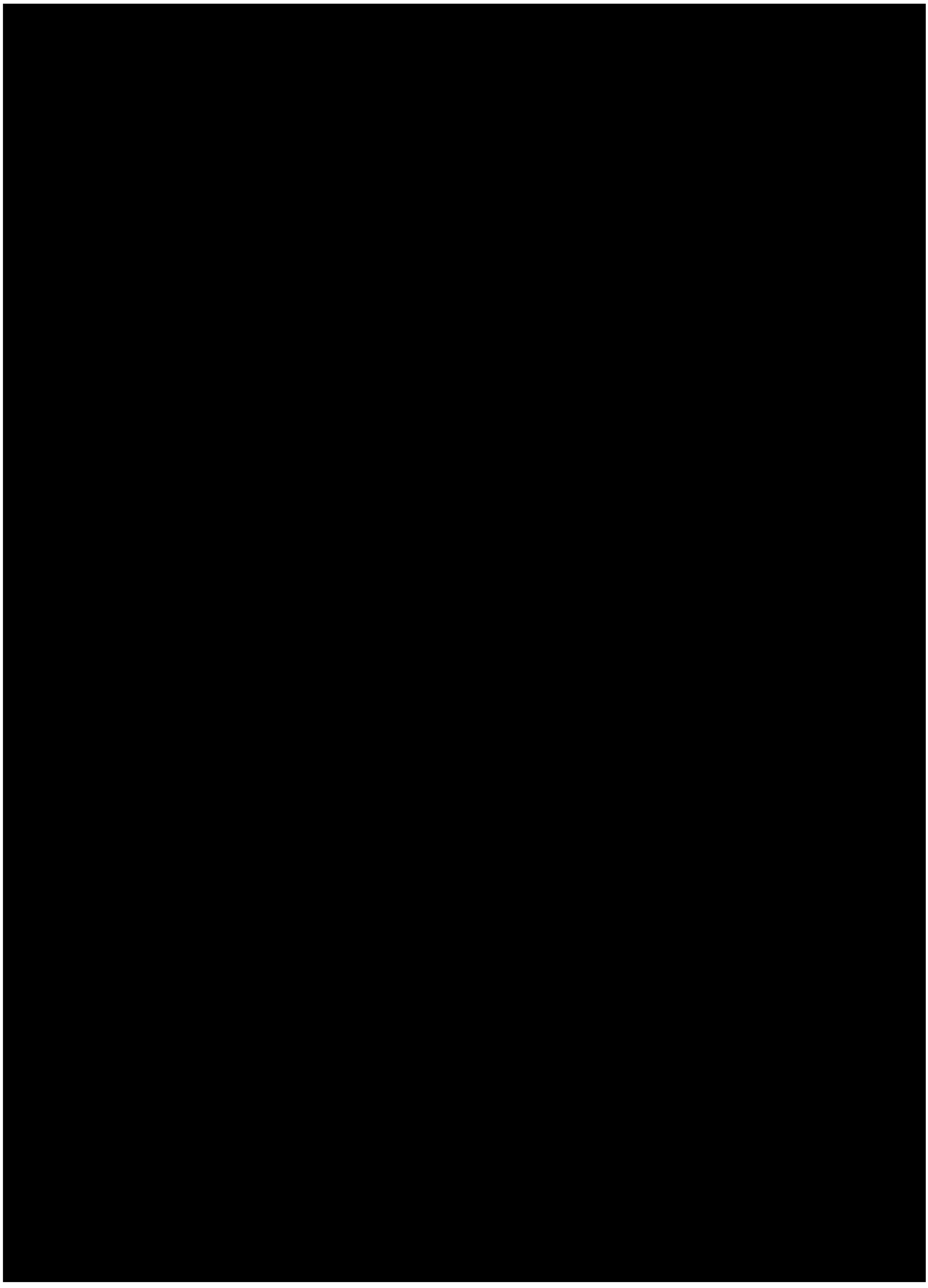


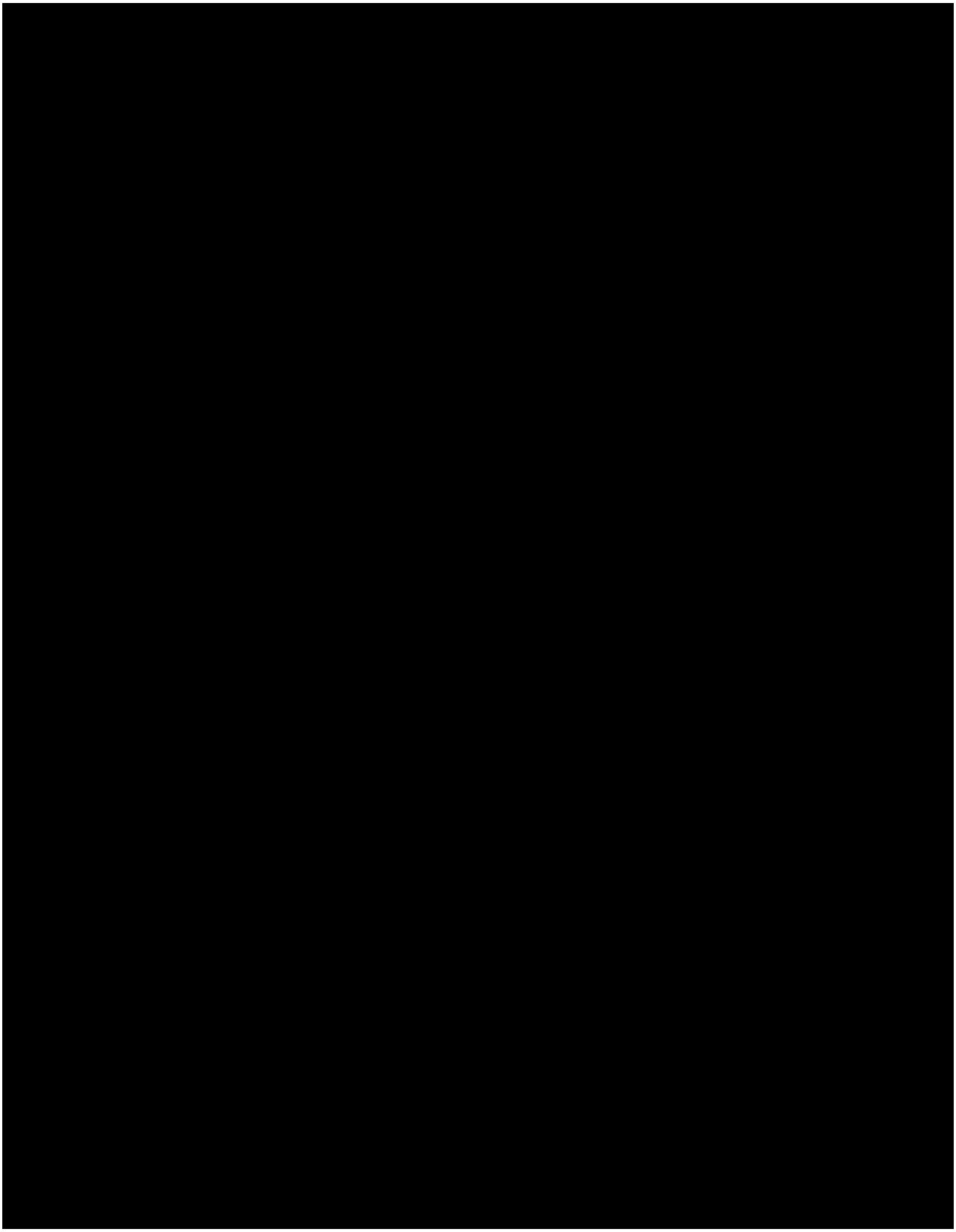


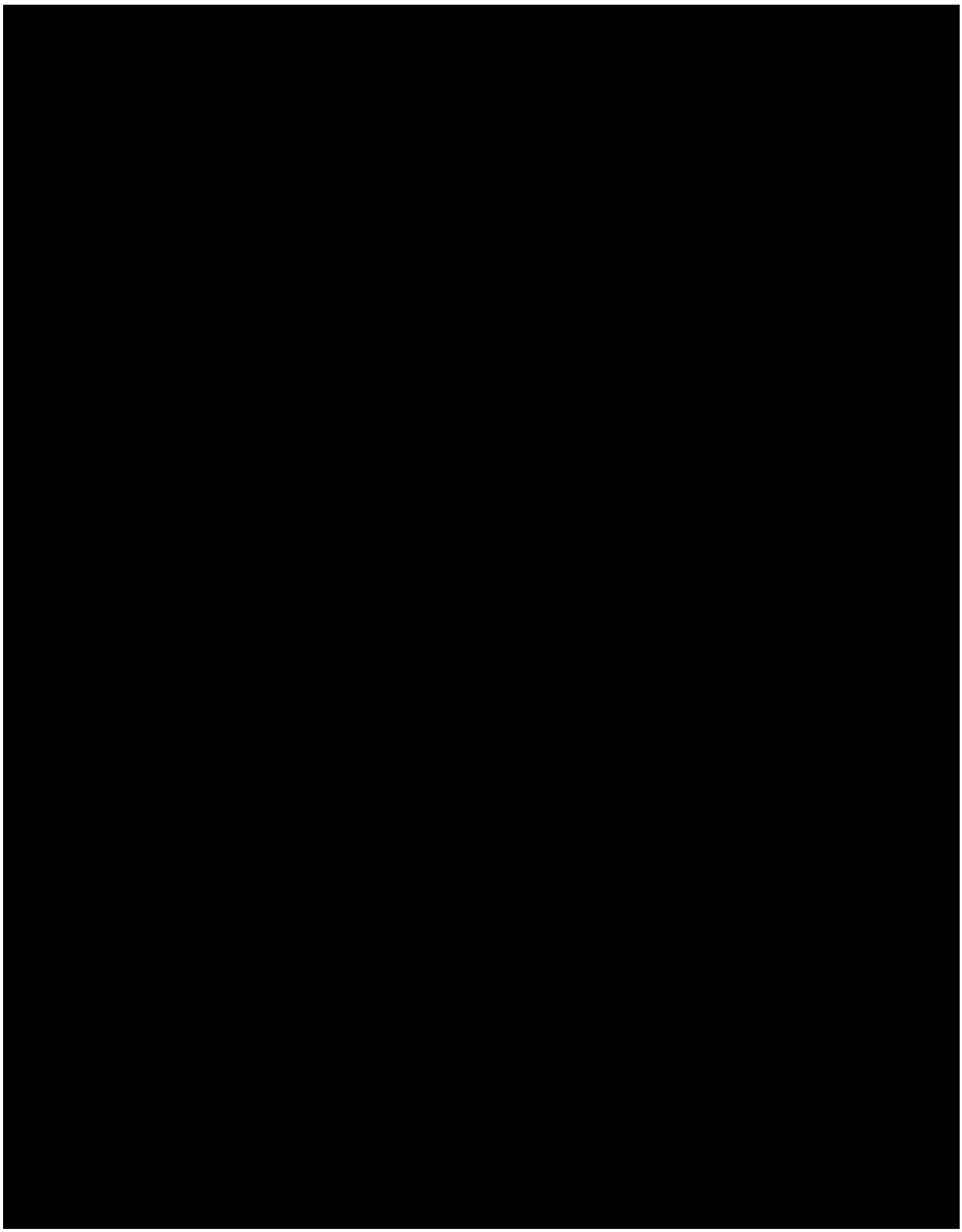


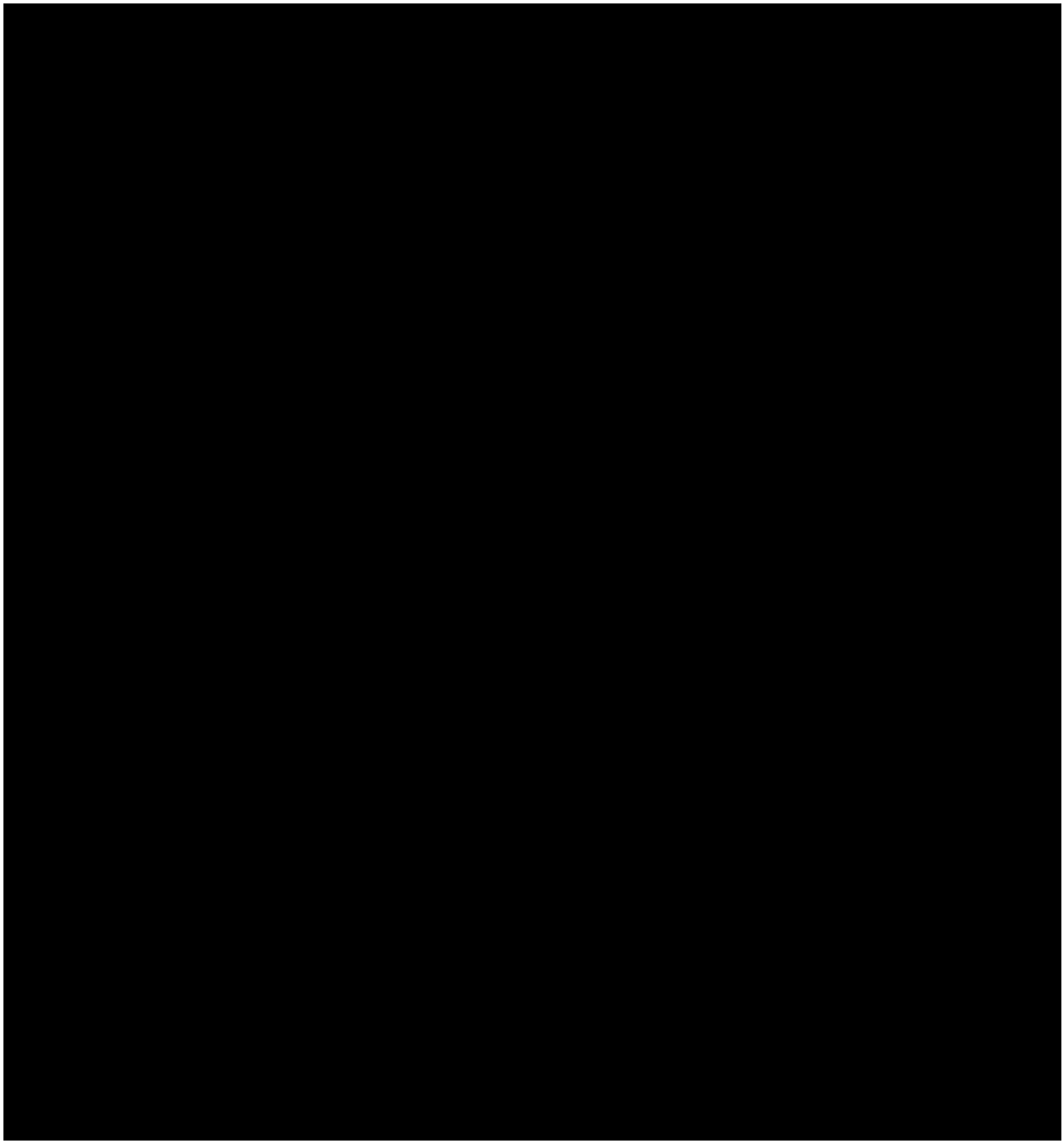


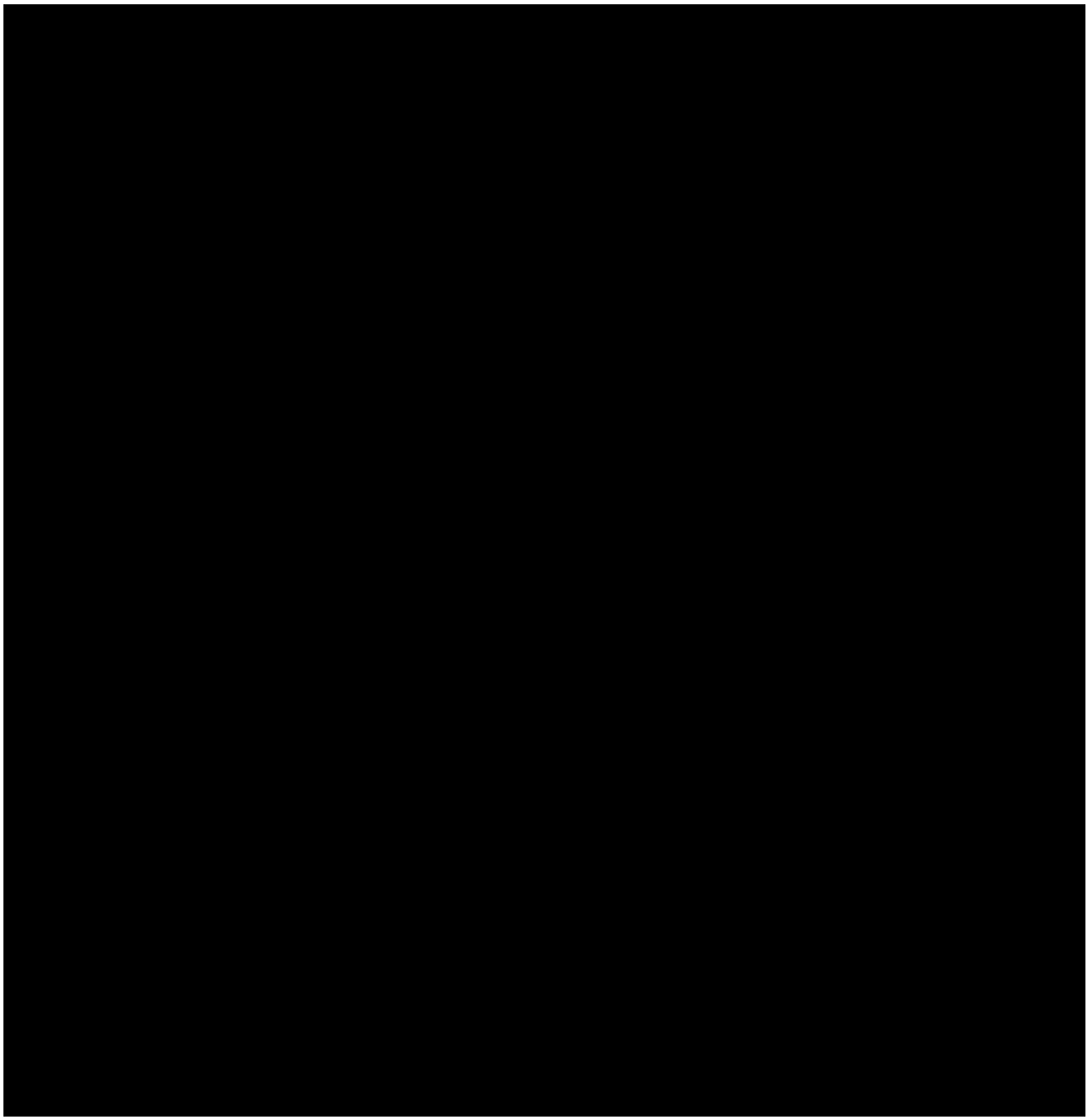












SCHEDULE 14 – KEY PERSONNEL

NOT USED

SCHEDULE 15 – EXIT PLAN

1 The Supplier shall, within three (3) months after the Commencement Date, deliver to the Authority an Exit Plan which:

1.1 sets out the Supplier's proposed methodology for achieving an orderly transition of the relevant Services from the Supplier to the Authority and/or its Replacement Supplier on the partial termination, expiry or termination of this Contract;

1.2 complies with the requirements set out in Paragraph 3; and

1.3 is otherwise reasonably satisfactory to the Authority.

2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within 20 Working Days of its submission, then such dispute shall be resolved in accordance with the dispute resolution procedure set out in Clause I1.

3 The Exit Plan shall set out, as a minimum:

3.1 how the Exit Information is obtained;

3.2 separate mechanisms for dealing with Ordinary Exit and Emergency Exit, the provisions relating to Emergency Exit being prepared on the assumption that the Supplier may be unable to provide the full level of assistance which is required by the provisions relating to Ordinary Exit, and in the case of Emergency Exit, provision for the supply by the Supplier of all such reasonable assistance as the Authority shall require to enable the Authority or its sub-contractors to provide the Services;

3.3 a mechanism for dealing with partial termination on the assumption that the Supplier will continue to provide the remaining Services under this Contract;

3.4 the management structure to be employed during both transfer and cessation of the Services in an Ordinary Exit and an Emergency Exit;

3.5 the management structure to be employed during the Termination Assistance Period;

3.6 a detailed description of both the transfer and cessation processes, including a timetable, applicable in the case of an Ordinary Exit and an Emergency Exit;

3.7 how the Services will transfer to the Replacement Supplier and/or the Authority, including details of the processes, documentation, data transfer,

systems migration, security and the segregation of the Authority's technology components from any technology components operated by the Supplier or its Sub-Contractors (where applicable);

3.8 a timetable and critical issues for providing the Termination Services;

3.9 subject to clause H9.3, any charges that would be payable for the provision of the Termination Services (calculated in accordance with the methodology that would apply if such Services were being treated as a Change), together with a capped estimate of such charges;

3.10 how the Termination Services would be provided (if required) during the Termination Assistance Period;

3.11 procedures to deal with requests made by the Authority and/or a Replacement Supplier for TUPE Information pursuant to paragraph 2.1 of Schedule 19; and

3.12 how each of the issues set out in this Schedule will be addressed to facilitate the transition of the Services from the Supplier to the Replacement Supplier and/or the Authority with the aim of ensuring that there is no disruption to or degradation of the Services during the Termination Assistance Period.

4 The Parties acknowledge that the migration of the Services from the Supplier to the Authority and/or its Replacement Supplier may be phased, such that certain of the Services are handed over before others.

5 The Supplier shall review and (if appropriate) update the Exit Plan on a basis consistent with the principles set out in this Schedule in the first month of each Contract Year (commencing with the second Contract Year) and if requested by the Authority following the occurrence of a Financial Distress Event, within 14 days of such request, to reflect any changes in the Services that have occurred since the Exit Plan was last agreed. Following such update, the Supplier shall submit the revised Exit Plan to the Authority for review. Within 20 Working Days following submission of the revised Exit Plan, the Parties shall meet and use reasonable endeavours to agree the contents of the revised Exit Plan. If the Parties are unable to agree the contents of the revised Exit Plan within that 20 Working Day period, such dispute shall be resolved in accordance with the dispute resolution procedure set out in Clause I1.

Finalisation of the Exit Plan

6 Within 20 Working Days after service of a termination notice by either Party or 6 months prior to the expiry of this Contract, the Supplier will submit for the Authority's approval the Exit Plan in a final form that could be implemented immediately. The final form of the Exit Plan shall be prepared on a basis

consistent with the principles set out in this Schedule and shall reflect any changes in the Services that have occurred since the Exit Plan was last agreed.

7 The Parties will meet and use their respective reasonable endeavours to agree the contents of the final form of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within 20 Working Days following its delivery to the Authority then such dispute shall be resolved in accordance with the dispute resolution procedure set out in Clause I1. Until the agreement of the final form of the Exit Plan, the Supplier shall provide the Termination Services in accordance with the principles set out in this Schedule and the last approved version of the Exit Plan (insofar as relevant).

Ministry of Justice

SCHEDULE 16 – POLICIES AND STANDARDS

1. INTRODUCTION

1.4 The Supplier shall at all times comply with the Policies and Standards listed in Annex A of this Schedule.

1.5 The Parties acknowledge that any standard, policy and/ or other document referred to within a Policy or Standard shall be deemed to form part of that Policy or Standard.

2. GENERAL

2.1 The Authority shall provide copies of the Policies and Standards from time to time to the Supplier upon request.

2.2 Throughout the Term, the Parties shall monitor and notify each other of any new or emergent policies or standards which could affect the Supplier's provision, or the Authority's receipt, of the Services.

2.3 Where a new or emergent standard is to be developed or introduced by the Authority, the Supplier shall be responsible for ensuring that the potential impact on the Suppliers provision, or the Authority's receipt, of the Services is explained to the Authority (in a reasonable timeframe), prior to the implementation of the new or emergent standard.

2.4 Where new versions of the Authority's Polices or Standards are developed and notified to the Supplier, the Supplier shall be responsible for ensuring that the potential impact on the Supplier's provision, or the Authority's receipt, of the Services is explained to the Authority (in a reasonable timeframe), prior to the implementation of the new version of the Policy or Standard, and the Supplier shall comply with such revised Policy or Standard (and any necessary Changes to this Contract shall be agreed in accordance with clause F4 (Change).

3. CONFLICTING POLICIES OR STANDARDS

3.1 Where Policies or Standards referenced conflict with each other or with Good Industry Practice, then the later Policy or Standard or best practice shall be adopted by the Supplier. Any such alteration to any Policy or Standard(s) shall require the prior written agreement of the Authority and shall be implemented within an agreed timescale.

Annex A Policies and Standards

National Standards for the Provision of Children's Advocacy Services, 2002
Independent Professional Advocacy – National Standards and Outcomes Framework for Children and Young People in Wales, 2019
Standards for children in the Youth Justice system, 2019
Healthcare Standards for Children and Young People in Secure Settings (Updated 2023)

Prison Service Instruction (PSI): Care and Management of Young People (Revised 2020)
Searching Policy Framework - GOV.UK (www.gov.uk)
Building Bridges: A Positive Behaviour Framework for the Children and Young People Secure Estate (Re-issued 2020)
Minimising and Managing Use of Separation and Isolation in the Children and Young People Secure Estate, 2020
The Young Offender Institution Rules 2000
The Secure Training Centre Rules
Crime and Disorder Act 1998

Error! Hyperlink reference not valid.
Wales Safeguarding Procedures
Safeguarding Vulnerable Groups Act 2006

Health and Care Act 2022
The Data Protection Act 2018
Children and Families Act 2014
Social Services and Well-being (Wales) Act 2014
Welsh Language (Wales) Measure 2011
Equality Act 2010
Mental Health Act 2007

Children Act 2004
Care Standards Act 2000
United Nations Convention on the Rights of the Child 1989
Human Rights Act 1998

SCHEDULE 17 – NOT USED

SCHEDULE 18 – AUTHORITY RESPONSIBILITIES

1 INTRODUCTION

1.1 The responsibilities of the Authority set out in this Schedule shall constitute the Authority Responsibilities under this Contract. Any obligations of the Authority in Schedule 1 (Specification) and shall not be Authority Responsibilities and the Authority shall have no obligation to perform any such obligations unless they are specifically stated to be "Authority Responsibilities" and included in the table in Paragraph 3.

1.2 The responsibilities specified within this Schedule shall be provided to the Supplier free of charge, unless otherwise agreed between the Parties.

2 GENERAL OBLIGATIONS

2.1 The Authority shall:

(a) perform those obligations of the Authority which are set out in the Clauses of this Contract and the Paragraphs of the Schedules (except Schedule 1 (Specification));

(b) use its reasonable endeavours to provide the Supplier with access to appropriate members of the Authority's staff, as such access is reasonably requested by the Supplier in order for the Supplier to discharge its obligations throughout the Term and the Termination Assistance Period;

(c) provide sufficient and suitably qualified Staff to fulfil the Authority's roles and duties under this Contract as defined in the Mobilisation Plan;

(d) use its reasonable endeavours to provide such documentation, data and/or other information that the Supplier reasonably requests that is necessary to perform its obligations under the terms of this Contract provided that such documentation, data and/or information is available to the Authority and is authorised for release by the Authority; and

(e) procure for the Supplier such agreed access and use of the Authority Premises (as a licensee only) and facilities (including relevant IT systems) as is reasonably required for the Supplier to comply with its obligations under this Contract, such access to be provided during the Authority's normal working hours on each Working Day or as otherwise agreed by the Authority (such agreement not to be unreasonably withheld or delayed).

3 SPECIFIC OBLIGATIONS (AUTHORITY RESPONSIBILITIES)

3.1 The Authority shall, in relation to this Contract perform the following Authority Responsibilities:

(a) The Authority shall provide the Supplier with reasonable access to the Children and Young People so as to enable the Supplier to carry out the Services, such access may entail physical access or access via digital means.

(b) The Authority shall, in accordance with security requirements and arrangements stipulated in this Contract and agreed locally with Secure Establishments (and as recorded in Local Protocols appended to Schedule 12) to the extent that physical access to the Premises is necessary to enable the Services to be carried out:

(i) undertake the security clearance checks necessary to enable each Advocate to provide the Services in respect of the relevant Secure Establishments; and

(ii) provide any keys (if required and permitted by the Authority and the relevant Secure Establishment) to enable the Advocates to access the relevant part of the Secure Establishment in order to provide the Services, and any necessary training, instruction or guidance to use these.

For the avoidance of doubt, the Authority Responsibility at (i) is to *undertake* the security clearance checks (where needed); the Supplier shall not be relieved of any Supplier Non-Performance resulting from any Advocate being refused clearance. It shall be the responsibility of the Supplier to select and vet Advocates, such that they reasonably believe that they will pass the Authority's clearance checks.

Ministry of Justice

SCHEDULE 19 – Staff Transfers

1 Entry Provisions

1.1 The Parties do not anticipate that TUPE will apply on the Commencement Date so as to give rise to the transfer of employees to the Supplier (as the Supplier is the incumbent provider of the Services).

1.2 Not used.

1.3 Not used.

1.4 The Supplier shall indemnify the Authority in full for and against all claims, costs, expenses, liabilities whatsoever and howsoever arising incurred or suffered by the Supplier including without limitation all legal expenses and other professional fees (together with any VAT thereon) in relation to:

1.4.1 any failure by the Supplier to comply with its obligations pursuant to TUPE.

1.4.2 Not used.

1.5 During the currency of this agreement the Supplier shall provide to the Authority any information that the Authority may reasonably require relating to any individual employed, assigned or engaged in providing the Services under this agreement (subject to applicable Data Protection Law).

2 Exit Provisions

2.1 No later than twelve (12) Months prior to the end of the Term, the Supplier shall fully and accurately disclose to the Authority all information the Authority may reasonably request in relation to the Staff including the following:

2.1.1 the total number of Staff whose employment/engagement terminates at the end of the Term, save for any operation of Law;

2.1.2 the age, gender, salary or other remuneration, future pay settlements and redundancy and pensions entitlement of the Staff referred to in paragraph 2.1.1 of this Schedule 19;

2.1.3 the terms and conditions of employment/engagement of the Staff referred to in paragraph 2.1.1 of this Schedule 19, their job titles and qualifications;

2.1.4 their immigration status;

2.1.5 details of any current disciplinary or grievance proceedings ongoing or circumstances likely to give rise to such proceedings and details of any claims current or threatened; and

2.1.6 details of all collective agreements with a brief summary of the current state of negotiations with any such bodies and with details of any current industrial disputes and claims for recognition by any trade union,

together the "**TUPE Information**".

2.2 At intervals determined by the Authority (which shall not be more frequent than once every thirty (30) days the Supplier shall give the Authority updated TUPE Information.

2.3 Each time the Supplier supplies TUPE Information to the Authority it warrants its completeness and accuracy and the Authority may assign the benefit of this warranty to any Replacement Supplier.

2.4 The Authority may use TUPE Information it receives from the Supplier for the purposes of TUPE and/or any retendering process in order to ensure an effective handover of all work in progress at the end of the Term. The Supplier shall provide the Replacement Supplier with such assistance as it shall reasonably request.

2.5 If TUPE applies to the transfer of the Services on termination of this Contract, the Supplier indemnifies and keeps indemnified the Authority, the Crown and any Replacement Supplier against all actions, suits, claims, demands, losses, charges, damages, costs and expenses and other liabilities which the Authority or the Crown or any Replacement Supplier may suffer or incur as a result of or in connection with:

2.5.1 the provision of TUPE Information;

2.5.2 any claim or demand by any Employee (whether in contract, tort or under statute) in each case arising directly or indirectly from any act, fault or omission of the Supplier or any Sub-Contractor in respect of any Employee on or before the end of the Term;

2.5.3 any failure by the Supplier or any Sub-Contractor to comply with its obligations under regulations 13 or 14 of TUPE or any award of compensation under regulation 15 of TUPE save where such failure arises from the failure of the Authority or a Replacement Supplier to comply with its duties under regulation 13 of TUPE;

2.5.4 any claim (including any individual employee entitlement under or consequent on such a claim) by any trade union or other body or person

representing any Employees arising from or connected with any failure by the Supplier or any Sub-Contractor to comply with any legal obligation to such trade union, body or person; and

2.5.5 any claim by any person who is transferred by the Supplier to the Authority and/or a Replacement Supplier whose name is not included in the list of Employees.

2.6 If the Supplier is aware that TUPE Employee Liability Information has become inaccurate or misleading, it shall notify the Authority and provide the Authority with up to date and accurate TUPE Information.

2.7 This paragraph 2 of Schedule 19 applies during the Term and indefinitely thereafter.

2.8 The Supplier undertakes to the Authority that, during the twelve (12) Months prior to the end of the Term the Supplier shall not (and shall procure that any Sub-Contractor shall not) without Approval (such Approval not to be unreasonably withheld or delayed):

2.8.1 amend or vary (or purport to amend or vary) the terms and conditions of employment or engagement (including, for the avoidance of doubt, pay) of any Staff (other than where such amendment or variation has previously been agreed between the Supplier and the Staff in the normal course of business and where any such amendment or variation is not in any way related to the transfer of the Services);

2.8.2 terminate or give notice to terminate the employment or engagement of any Staff (other than in circumstances in which the termination is for reasons of misconduct or lack of capability);

2.8.3 transfer away, remove, reduce or vary the involvement of any other Staff from or in the provision of the Services (other than where such transfer or removal: (i) was planned as part of the individual's career development; (ii) takes place in the normal course of business; and (iii) will not have any adverse impact upon the delivery of the Services by the Supplier, (provided that any such transfer, removal, reduction or variation is not in any way related to the transfer of the Services)); or

2.8.4 recruit or bring in any new or additional individuals to provide the Services who were not already involved in providing the Services prior to the relevant period.

Ministry of Justice

IN WITNESS of which this Contract is duly executed by the Parties on the date which appears at the head of page 1.

SIGNED for and on behalf of the
Secretary of State for Justice

Signature: [redacted]

Name (block capitals): [redacted]

Position: Associate Commercial Specialist

Date: Feb 19, 2024

SIGNED for and on behalf of
BARNARDO'S

Signature: [redacted]

Name (block capitals): [redacted]

Position: Director Children's Services

Date: Feb 19, 2024