

Contract (Short Form – Services)

Contract for the provision of MNSI Anti Racism Training

Contract Reference CQC MNSI 008

April 2025

Contents

1	Interpretation.....	5
2	Priority of documents	10
3	Supply of Services	10
4	Term	11
5	Price, Payment and Recovery of Sums Due.....	11
6	Premises and equipment	12
7	Staff and Key Personnel	13
8	Assignment and sub-contracting.....	14
9	Intellectual Property Rights	15
10	Governance and Records.....	16
11	Confidentiality, Transparency and Publicity	16
12	Freedom of Information	18
13	Protection of Data.....	18
13A	Security	19
14	Liability and Insurance.....	20
15	Force Majeure	21
16	Termination	22
17	Compliance	23
18	Prevention of Fraud, Corruption and Bribery	24
19	Dispute Resolution	25
20	General.....	25
21	Notices	27
22	Governing Law and Jurisdiction	28
23	TUPE.....	28

SCHEDULE 1 –SPECIFICATION.....30

SCHEDULE 2 – TENDER RESPONSE.....35

SCHEDULE 3 – PRICE66

SCHEDULE 4 – PROCESSING, PERSONAL DATA AND DATA SUBJECTS.....75

SCHEDULE 5 – SECURITY REQUIREMENTS AND PLAN.....81

SCHEDULE 6 – CHANGE CONTROL.....95

SCHEDULE 7 – THIRD PARTY SOFTWARE97

SCHEDULE 8 – EXIT MANAGEMENT STRATEGY.....98

PARTIES

- (1) **CARE QUALITY COMMISSION** of Citygate, Gallowgate, Newcastle Upon Tyne, NE1 4PA (“**Authority**”)
 - and
 - (2) **MISSION DIVERSE CONSULTING LTD**, 12 Pheonix Business Park, Onyx House, Birmingham, B7 4NU Company registration 12985865 (“**Contractor**”)
- (Together the “**Parties**”)

Background

1. The Authority is the independent health and social care regulator in England that monitors, inspects and regulates health and social care services to ensure they meet fundamental standards of quality and safety. It ensures health and social care services provide people with safe, effective, compassionate, high-quality care and we encourage care services to improve.
2. In order to provide MNSI team Anti Racism Training.
3. The Contractor has been appointed by the Authority to provide the Services.
4. Therefore, the Parties have agreed to enter into this Contract for the provision of the services defined in the Specification.

1 Interpretation

1.1 In these terms and conditions:

“Approval”	means the written consent of the Authority;
“Authority”	means the Care Quality Commission;
“Authority Data”	means: <ul style="list-style-type: none">(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, tangible media, and which are: (i) supplied to the Contractor by or on behalf of the Authority; or (ii) which the Contractor is required to generate, transmit pursuant to the Contract; or(b) any Personal Data for which the Authority is the Data Controller;
“Award Letter”	means the letter from the Authority to the Contractor containing these terms and conditions;
“Anti-Slavery and Human Trafficking Laws”	means all applicable anti-slavery and human trafficking laws, statutes, regulations, policies and codes from time to time in force including but not limited to the Modern Slavery Act 2015;
“Breach of Security”	means the occurrence of unauthorised access to or use of the Premises, the Premises, the Services, the Contractor system, or any ICT or data (including Authority Data) used by the Authority or the Contractor in connection with the Contract;
“Central Government Body”	means a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics: <ul style="list-style-type: none">(a) Government Department;(b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive(c) Non-Ministerial Department; or(d) Executive Agency;
“Change Control Notice (“CCN”)”	means a change control notice in the form set out in Schedule 6;
“Contract”	means the contract consisting of these terms and conditions, any attached Schedules, the invitation to tender including Specification, the Tender Response and Award Letter between the Authority the Contractor;
“Contract Period”	shall mean the Term of the Contract;

“Confidential Information”	means all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which (i) is known by the receiving Party to be confidential; (ii) is marked as or stated to be confidential; or (iii) ought reasonably to be considered by the receiving Party to be confidential;
“Contractor”	means the person named as Contractor who was awarded this contract;
“Contractor’s response”	means the document submitted by the Contractor to the Authority in response to the Authority’s invitation to suppliers for formal offers to supply the Services appended hereto in Schedule 3;
“Contractor System”	means the information and communications technology system used by the Contractor in performing the Services including the Software, the Contractor Equipment and related cabling (but excluding the Authority System);
“Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Data Protection Officer”	shall each have the same meaning given in the GDPR;
“Data Protection Legislation”	means (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time; (ii) the DPA 2018 subject to Royal Assent to the extent that it relates to the processing of Personal Data and privacy; (iii) all applicable Law about the processing of Personal Data and privacy;
“Data Loss Event”	means any event that results, or may result, in unauthorised access to Personal Data held by the Contractor under this Contract and/or actual or potential loss and/or destruction breach of this Contract, including any Personal Data Breach;
“Data Protection Impact Assessment”	means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;
“Data Subject Request”	means a request made by or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access his or her Personal Data;
“DPA”	means the Data Protection Act 2018 and any subordinate legislation made under that Act from time to time together with any guidance and/or codes of practice issued by the Commissioner or relevant government department in relation to such legislation;
“Default”	means any breach of the obligations of the relevant Party (including abandonment of the 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 the Contract and in respect of which such Party is liable to the other;
“Expiry Date”	means the date for expiry of the Contract as set out in the Award Letter;

“FOIA”	means the Freedom of Information Act 2000;
“GDPR”	means the General Data Protection Regulation (<i>Regulation (EU) 2016/679</i> ;
“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 under the same or similar circumstances;
“Information”	has the meaning given under section 84 of the FOIA;
“Key Personnel”	means any persons specified as such in the Specification or Contract otherwise notified as such by the Authority to the Contractor in writing;
“Law”	means any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or judgment of a relevant court of law, or directives or requirements of any Regulatory Body with which the Contractor is bound to comply;
“LED”	means Law Enforcement Directive (<i>Directive (EU) 2016/680</i>)
“Loss”	means any losses, costs, price, expenses, interest, fees (including legal fees), payments, demands, liabilities, claims, proceedings, actions, penalties, price, fines, damages, destruction, adverse judgments, orders or other sanctions and the term “ Losses ” shall be construed; accordingly,
“Party”	means the Contractor or the Authority (as appropriate) and “Parties” shall mean both of them;
“Premises”	means the location where the Services are to be supplied, as set out in the Specification;
“Price”	means the price (excluding any applicable VAT) payable to the Contractor by the Authority under the Contract, as set out in Schedule 3 for the full and proper performance by the Contractor of its obligations under the Contract;
“Pricing Schedule”	means Schedule 3 containing details of the Price;
“Processing”	has the meaning given to it in the Data Protection Legislation but, for the purposes of the Contract, it shall include both manual and automatic processing and "Process" and "Processed" shall be interpreted; accordingly,
“Processor Personnel”	means all directors, officer, employees, agents, consultants and contractors of the Processor engaged in the performance of its obligations under this Contract;
“Prohibited Act”	means: <ul style="list-style-type: none"> (a) to directly or indirectly offer, promise or give any person working for or engaged by the Authority a financial or other advantage to: <ul style="list-style-type: none"> 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

(c) advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with the Contract;

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

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 which include: pseudonymising 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 such measures adopted by it including those outlined in Schedule 5 (Security Requirements and Plan);
"Purchase Order Number"	means the Authority's unique number relating to the supply of the Services by the Contractor to the Authority in accordance with the terms of the Contract;
"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;
"Replacement Contractor"	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 the Contract;
"Request for Information"	has the meaning set out in the FOIA or the Environmental Information Regulations 2004 as relevant (where the meaning set out for the term "request" shall apply);
"Schedule"	means a schedule attached to, and forming part of, the Contract;
"Security Plan"	means the Contractor's security plan prepared pursuant to paragraph 3 of Schedule 5 (Security Requirements and Plan), an outline of which is set out in an Appendix to Schedule 5
"Security Policy Framework"	means the HMG Security Policy Framework (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61111/Security-Policy-Framework-v1.1.doc.pdf)
"Services"	means the services to be supplied by the Contractor to the Authority under the Contract as set out in Schedule 1;
"Specification"	means the specification for the Services (including as to quantity, description and quality) Award Letter and appended hereto in Schedule 1;
"Staff"	means all directors, officers, employees, agents, consultants and contractors of the Contractor and/or of any sub-contractor of the Contractor engaged in the performance obligations under the Contract;

“Staff Vetting Procedures”	means vetting procedures that accord with good industry practice or, where requested by the Authority, the Authority’s procedures for the vetting of personnel as provided to the Contractor from time to time;
“Sub–Contractor”	means a third party directly or indirectly contracted to the Contractor (irrespective of whether such person is an agent or company within the same group of companies as the Contractor) whose services are used by the Contractor (either directly or indirectly) in provision of the Services, and “ Sub-Contract ” shall be construed; accordingly,
“Sub-processor”	means any third Party appointed to process Personal Data on behalf of the Processor related
“Supplier Code of Conduct”	means the HM Government Contractor Code of Conduct dated September 2017;
“Term”	means the period from the start date of the Contract set out in the Award Letter to the Expiry Date as such period may be extended in accordance with clause 4.2 or terminated in accordance with the terms and conditions of the Contract;
“Third Party Software”	means software which is proprietary to any third party which is or will be used by the Contractor to provide the Services including the software and which is specified as such in Schedule 7;
“TUPE”	means the Transfer of Undertakings (Protection of Employment) Regulations 2006;
“VAT”	means value added tax in accordance with the provisions of the Value Added Tax Act 1994; and
“Variation”	means a variation to the Specification, the Price or any of the terms and conditions of the Contract;
“Working Day”	means a day (other than a Saturday or Sunday) on which banks are open for business in the City of London.

1.2 In these terms and conditions, unless the context otherwise requires:

- 1.2.1 references to numbered clauses are references to the relevant clause in these terms and conditions;
- 1.2.2 any obligation on any Party not to do or omit to do anything shall include an obligation not to allow that thing to be done or omitted to be done;
- 1.2.3 the headings to the clauses of these terms and conditions are for information only and do not affect the interpretation of the Contract;
- 1.2.4 any reference to an enactment includes reference to that enactment as amended or replaced from time to time and to any subordinate legislation or byelaw made under that enactment; and
- 1.2.5 the word ‘including’ shall be understood as meaning ‘including without limitation’.

2 Priority of documents

2.1 In the event of, and only to the extent of, any conflict between the clauses of the Contract, any document referred to in those clauses and the Schedules, the conflict shall be resolved in accordance with the following order of precedence:

- a) these terms and conditions
- b) the Schedules
- c) any other document referred to in these terms and conditions

3 Supply of Services

3.1 In consideration of the Authority's agreement to pay the Price, the Contractor shall supply the Services to the Authority for the Term subject to and in accordance with the terms and conditions of the Contract.

3.2 In supplying the Services, the Contractor shall:

3.2.1 co-operate with the Authority in all matters relating to the Services and comply with all the Authority's instructions;

3.2.2 perform the Services with all reasonable care, skill and diligence in accordance with good industry practice in the Contractor's industry, profession or trade;

3.2.3 use Staff who are suitably skilled, experienced and possess the required qualifications to perform tasks assigned to them, and in sufficient number to ensure that the Contractor's obligations are fulfilled in accordance with the Contract;

3.2.4 ensure that the Services shall conform with all descriptions and specifications set out in the Specification;

3.2.5 comply with all applicable laws; and

3.2.6 provide all equipment, tools and vehicles and other items as are required to provide the Services.

3.3 The Authority may by written notice to the Contractor at any time request a Variation to the scope of the Services. If the Contractor agrees to any Variation to the scope of the Services, the Price shall be subject to fair and reasonable adjustment to be agreed in writing between the Authority and the Contractor.

3.4 Any Variation will not take effect unless recorded in a Change Control Notice in the form set out in Schedule 6 and approved in writing by the Authority.

4 Term

- 4.1 The Contract shall take effect on 14th April 2025 and shall expire on 31st March 2027, unless it is otherwise extended in accordance with clause 4.2 or terminated in accordance with the terms and conditions of the Agreement.
- 4.2 The Authority may extend the Contract for a period of up to 12 months by giving not less than 3 months' notice in writing to the Contractor prior to the Expiry Date. The terms and conditions of the Contract shall apply throughout any such extended period.

5 Price, Payment and Recovery of Sums Due

- 5.1 The Price for the Services shall be as set out in Schedule 2 and shall be the full and exclusive remuneration of the Contractor in respect of the supply of the Services. Unless otherwise agreed in writing by the Authority, the Price shall include every cost and expense of the Contractor directly or indirectly incurred in connection with the performance of the Services.
- 5.2 The Contractor shall invoice the Authority as specified in Schedule 2. Each invoice shall include such supporting information required by the Authority to verify the accuracy of the invoice, including the relevant Purchase Order Number and a breakdown of the Services supplied in the invoice period.
- 5.3 In consideration of the supply of the Services by the Contractor, the Authority shall pay the Contractor the invoiced amounts no later than 30 days after receipt of a valid invoice which includes a valid Purchase Order Number. The Authority may, without prejudice to any other rights and remedies under the Contract, withhold or reduce payments in the event of unsatisfactory performance.
- 5.4 All amounts stated are exclusive of VAT which shall be charged at the prevailing rate. The Authority shall, following the receipt of a valid VAT invoice, pay to the Contractor a sum equal to the VAT chargeable in respect of the Services.
- 5.5 If there is a dispute between the Parties as to the amount invoiced, the Authority shall pay the undisputed amount. The Contractor shall not suspend the supply of the Services unless the Contractor is entitled to terminate the Contract for a failure to pay undisputed sums in accordance with clause 16.4. Any disputed amounts shall be resolved through the dispute resolution procedure detailed in clause 19.
- 5.6 If a payment of an undisputed amount is not made by the Authority by the due date, then the Authority shall pay the Contractor interest at the interest rate specified in the Late Payment of Commercial Debts (Interest) Act 1998.
- 5.7 If any sum of money is recoverable from or payable by the Contractor under the Contract (including any sum which the Contractor is liable to pay to the Authority in respect of any breach of the Contract), that sum may be deducted unilaterally by the Authority from any sum then due, or which may come due, to the Contractor under the Contract or under any other agreement or contract with the Authority. The Contractor shall not be entitled to assert any credit, set-off or counterclaim against

the Authority in order to justify withholding payment of any such amount in whole or in part.

5.8 Where the Contractor enters into a sub-contract, the Contractor shall include in that sub-contract:

5.8.1 Provisions having the same effect as clauses 5.2 to 5.6 of the Contract and

5.8.2 Provisions requiring the counterparty to that subcontract to include in any sub-contract which it awards provisions having the same effect as clauses 5.2 to 5.6 of this Contract.

5.8.3 In this clause 5.8 'sub-contract' means a contract between two or more Contractors, 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.

6 Premises and equipment

6.1 If necessary, the Authority shall provide the Contractor with reasonable access at reasonable times to its premises for the purpose of supplying the Services. All equipment, tools and vehicles brought onto the Authority's premises by the Contractor, or the Staff shall be at the Contractor's risk.

6.2 If the Contractor supplies all or any of the Services at or from the Authority's premises, on completion of the Services or termination or expiry of the Contract (whichever is the earlier) the Contractor shall vacate the Authority's premises, remove the Contractor's plant, equipment and unused materials and all rubbish arising out of the provision of the Services and leave the Authority's premises in a clean, safe and tidy condition. The Contractor shall be solely responsible for making good any damage to the Authority's premises or any objects contained on the Authority's premises which is caused by the Contractor or any Staff, other than fair wear and tear.

6.3 If the Contractor supplies all or any of the Services at or from its premises or the premises of a third party, the Authority may, during normal business hours and on reasonable notice, inspect and examine the manner in which the relevant Services are supplied at or from the relevant premises.

6.4 The Authority shall be responsible for maintaining the security of its premises in accordance with its standard security requirements. While on the Authority's premises the Contractor shall, and shall procure that all Staff shall, comply with all the Authority's security requirements.

6.5 Where all or any of the Services are supplied from the Contractor's premises, the Contractor shall, at its own cost, comply with all security requirements specified by the Authority in writing.

6.6 Without prejudice to clause 3.2.6, any equipment provided by the Authority for the purposes of the Contract shall remain the property of the Authority and shall be used

by the Contractor and the Staff only for the purpose of carrying out the Contract. Such equipment shall be returned promptly to the Authority on expiry or termination of the Contract.

- 6.7 The Contractor shall reimburse the Authority for any loss or damage to the equipment (other than deterioration resulting from normal and proper use) caused by the Contractor or any Staff. Equipment supplied by the Authority shall be deemed to be in a good condition when received by the Contractor or relevant Staff unless the Authority is notified otherwise in writing within 5 Working Days.
- 6.8 Any Premises/land made available from time to time to the Contractor by the Authority in connection with the contract, shall be made available to the contractor on a non-exclusive licence basis free of charge and shall be used by the contractor solely for the purpose of performing its obligations under the contract. The Contractor shall have the use of such Premises/land as licensee and shall vacate the same on completion, termination or abandonment of the Contract.
- 6.9 The Parties agree that there is no intention on the part of the Authority to create a tenancy of any nature whatsoever in favour of the Contractor or its Staff and that no such tenancy has or shall come into being and, notwithstanding any rights granted pursuant to the Contract, the Authority retains the right at any time to use any premises owned or occupied by it in any manner it sees fit.
- 6.10 Should the Contractor require modifications to the Premises, such modifications shall be subject to prior Approval and shall be carried out by the Authority at the Contractor's expense. The Authority shall undertake approved modification work without undue delay. Ownership of such modifications shall rest with the Authority.
- 6.11 All the Contractor's equipment shall remain at the sole risk and responsibility of the Contractor, except that the Authority shall be liable for loss of or damage to any of the Contractor's property located on Authority's Premises which is due to the negligent act or omission of the Authority.

7 Staff and Key Personnel

- 7.1 If the Authority reasonably believes that any of the Staff are unsuitable to undertake work in respect of the Contract, it may, by giving written notice to the Contractor:
 - 7.1.1 refuse admission to the relevant person(s) to the Authority's premises;
 - 7.1.2 direct the Contractor to end the involvement in the provision of the Services of the relevant person(s); and/or
 - 7.1.3 require that the Contractor replace any person removed under this clause with another suitably qualified person and procure that any security pass issued by the Authority to the person removed is surrendered,and the Contractor shall comply with any such notice.
- 7.2 The Contractor shall:

- 7.2.1 ensure that all Staff are vetted in accordance with the Staff Vetting Procedures; and if requested, comply with the Authority's Staff Vetting Procedures as supplied from time to time;
- 7.2.2 if requested, provide the Authority with a list of the names and addresses (and any other relevant information) of all persons who may require admission to the Authority's premises in connection with the Contract;
- 7.2.3 procure that all Staff comply with any rules, regulations and requirements reasonably specified by the Authority; and
- 7.2.4 shall at all times comply with the Supplier Code of Conduct (<https://www.gov.uk/government/publications/Contractor-code-of-conduct>).
- 7.2.5 ensure that it does not engage in any act or omission that would contravene Anti-Slavery and Human Trafficking Laws.
- 7.3 Any Key Personnel shall not be released from supplying the Services without the agreement of the Authority, except by reason of long-term sickness, maternity leave, paternity leave, termination of employment or other extenuating circumstances.
- 7.4 Any replacements to the Key Personnel shall be subject to the prior written agreement of the Authority (not to be unreasonably withheld). Such replacements shall be of at least equal status or of equivalent experience and skills to the Key Personnel being replaced and be suitable for the responsibilities of that person in relation to the Services.
- 7.5 At the Authority's written request, the Contractor shall provide a list of names and addresses of all persons who may require admission in connection with the Contract to the Premises, specifying the capacities in which they are concerned with the Contract and giving such other particulars as the Authority may reasonably request.
- 7.6 The Contractor's Staff, engaged within the boundaries of the Premises shall comply with such rules, regulations and requirements (including those relating to security arrangements) as may be in force from time to time for the conduct of personnel when at or outside the Premises.
- 7.7 The Authority may require the Contractor to ensure that any person employed in the provision of the Services has undertaken a Criminal Records Bureau check as per the Staff Vetting Procedures.

8 Assignment and sub-contracting

- 8.1 The Contractor shall not without the written consent of the Authority assign, sub-contract, novate or in any way dispose of the benefit and/ or the burden of the Contract or any part of the Contract. The Authority may, in the granting of such consent, provide for additional terms and conditions relating to such assignment, sub-contract, novation or disposal. The Contractor shall be responsible for the acts and omissions of its sub-contractors as though those acts and omissions were its own.

- 8.2 If the Contractor enters into a Sub-Contract for the purpose of performing its obligations under the Contract, it shall ensure that a provision is included in such sub-contract which requires payment to be made of all sums due by the Contractor to the Sub-Contractor within a specified period not exceeding 30 days from the receipt of a valid invoice.
- 8.3 If the Authority has consented to the placing of Sub-Contracts, the Contractor shall:
- (a) impose obligations on its Sub-Contractor on the same terms as those imposed on it pursuant to this Contract and shall procure that the Sub-Contractor complies with such terms; and
 - (b) provide a copy at no charge to the Authority, of any Sub-Contract, on receipt of a request for such by the Authority.
- 8.4 The Authority may assign, novate, or otherwise dispose of its rights and obligations under the Contract without the consent of the Contractor provided that such assignment, novation or disposal shall not increase the burden of the Contractor's obligations under the Contract.

9 Intellectual Property Rights

- 9.1 All intellectual property rights in any materials provided by the Authority to the Contractor for the purposes of this Contract shall remain the property of the Authority but the Authority hereby grants the Contractor a royalty-free, non-exclusive and non-transferable licence to use such materials as required until termination or expiry of the Contract for the sole purpose of enabling the Contractor to perform its obligations under the Contract.
- 9.2 All Intellectual Property rights in any guidance, specifications, instructions, toolkits, plans, data, drawings, databases, patents, patterns, models, designs or other materials (intellectual property) prepared by or for the Contractor furnished to or made available to the Authority for use, or intended use, in relation to the performance by the Contractor of its obligations under the Contract shall belong to the Contractor; and All Intellectual Property Rights in the Contractor's Intellectual Property Materials shall remain the property of the Contractor or its licensors, and the Authority shall not, and shall ensure that its staff shall not (except insofar as is necessary in order for the Authority to exercise its rights and to take the benefit of this Contract, including the Services provided under the Contract, or as is otherwise permitted under the Contract) without prior approval, use or disclose any Intellectual Property Rights in the Contractor's Intellectual Property Materials.
- 9.3 The Contractor hereby grants the Authority:
- a) A royal-free and non-exclusive licence to use the materials created duration of this contract which the Authority reasonably requires for it to exercise its rights and take the benefit of this Contract.
- 9.4 The Contractor shall indemnify, and keep indemnified, the Authority in full against all costs, expenses, damages and losses (whether direct or indirect), including any interest, penalties, and reasonable legal and other professional fees awarded

against or incurred or paid by the Authority as a result of or in connection with any claim made against the Authority for actual or alleged infringement of a third party's intellectual property arising out of, or in connection with, the supply or use of the Services, to the extent that the claim is attributable to the acts or omission of the Contractor its Staff, agents or sub-contractors.

- 9.5 The Authority shall promptly notify the Contractor of any infringement claim made against it relating to any Services and, subject to any statutory obligation requiring the Authority to respond, shall permit the Contractor to have the right, at its sole discretion to assume, defend, settle or otherwise dispose of such claim. The Authority shall give the Contractor such assistance as it may reasonably require to dispose of the claim and shall not make any statement which might be prejudicial to the settlement or defence of the claim.

10 Governance and Records

- 10.1 The Contractor shall:

10.1.1 attend progress meetings with the Authority at the frequency and times specified by the Authority and shall ensure that its representatives are suitably qualified to attend such meetings; and

10.1.2 submit progress reports to the Authority at the times and in the format specified by the Authority.

- 10.2 The Contractor shall keep and maintain until 6 years after the end of the Contract, or as long a period as may be agreed between the Parties, full and accurate records of the Contract including the Services supplied under it and all payments made by the Authority. The Contractor shall on request afford the Authority or the Authority's representatives such access to those records as may be reasonably requested by the Authority in connection with the Contract.

11 Confidentiality, Transparency and Publicity

- 11.1 Subject to clause 11.2, each Party shall:

11.1.1 treat all Confidential Information it receives as confidential, safeguard it accordingly and not disclose it to any other person without the prior written permission of the disclosing Party; and

11.1.2 not use or exploit the disclosing Party's Confidential Information in any way except for the purposes anticipated under the Contract.

- 11.2 Notwithstanding clause 11.1, a Party may disclose Confidential Information which it receives from the other Party:

11.2.1 where disclosure is required by applicable law or by a court of competent jurisdiction;

11.2.2 to its auditors or for the purposes of regulatory requirements;

- 11.2.3 on a confidential basis, to its professional advisers;
- 11.2.4 to the Serious Fraud Office where the Party has reasonable grounds to believe that the other Party is involved in activity that may constitute a criminal offence under the Bribery Act 2010;
- 11.2.5 where the receiving Party is the Contractor, to the Staff on a need to know basis to enable performance of the Contractor's obligations under the Contract provided that the Contractor shall procure that any Staff to whom it discloses Confidential Information pursuant to this clause 11.2.5 shall observe the Contractor's confidentiality obligations under the Contract; and
- 11.2.6 where the receiving Party is the Authority:
 - a) on a confidential basis to the employees, agents, consultants and contractors of the Authority;
 - b) on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company to which the Authority transfers or proposes to transfer all or any part of its business;
 - c) to the extent that the Authority (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions; or
 - d) in accordance with clause 12.

and for the purposes of the foregoing, references to disclosure on a confidential basis shall mean disclosure subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the Authority under this clause 11.

- 11.3 The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of the Contract is not Confidential Information and the Contractor hereby gives its consent for the Authority to publish this Contract in its entirety to the general public (but with any information that is exempt from disclosure in accordance with the FOIA redacted) including any changes to the Contract agreed from time to time. The Authority may consult with the Contractor to inform its decision regarding any redactions but shall have the final decision in its absolute discretion whether any of the content of the Contract is exempt from disclosure in accordance with the provisions of the FOIA.
- 11.4 The Contractor shall not, and shall take reasonable steps to ensure that the Staff shall not, make any press announcement or publicise the Contract or any part of the Contract in any way, except with the prior written consent of the Authority.

12 Freedom of Information

- 12.1 The Contractor acknowledges that the Authority is subject to the requirements of the FOIA and the Environmental Information Regulations 2004 and shall and procure that any sub-contractor shall:
 - 12.1.1 provide all necessary assistance and cooperation as reasonably requested by the Authority to enable the Authority to comply with its obligations under the FOIA and the Environmental Information Regulations 2004;
 - 12.1.2 transfer to the Authority all Requests for Information relating to this Contract that it receives as soon as practicable and in any event within 2 Working Days of receipt;
 - 12.1.3 provide the Authority with a copy of all Information belonging to the Authority requested in the Request for Information which is in its possession or control in the form that the Authority requires within 5 Working Days (or such other period as the Authority may reasonably specify) of the Authority's request for such Information; and
 - 12.1.4 not respond directly to a Request for Information unless authorised in writing to do so by the Authority.
- 12.2 The Contractor acknowledges that the Authority may be required under the FOIA and the Environmental Information Regulations 2004 to disclose Information concerning the Contractor or the Services (including commercially sensitive information) without consulting or obtaining consent from the Contractor. In these circumstances the Authority shall, in accordance with any relevant guidance issued under the FOIA, take reasonable steps, where appropriate, to give the Contractor advance notice, or failing that, to draw the disclosure to the Contractor's attention after any such disclosure.
- 12.3 Notwithstanding any other provision in the Contract, the Authority shall be responsible for determining in its absolute discretion whether any Information relating to the Contractor or the Services is exempt from disclosure in accordance with the FOIA and/or the Environmental Information Regulations 2004.

13 Protection of Data

13.1 Authority Data

- 13.1.1 The Contractor shall not delete or remove any proprietary notices contained within or relating to the Authority Data.
- 13.1.2 The Contractor shall not store, copy, disclose, or use the Authority Data except as necessary for the performance by the Contractor of its obligations under this Contract or as otherwise expressly authorised in writing by the Authority.

- 13.1.3 To the extent that Authority Data is held and/or Processed by the Contractor, the Contractor shall supply Authority Data to the Authority as requested by the Authority in the format specified in the Specification.
- 13.1.4 The Contractor shall preserve the integrity of Authority Data and prevent the corruption or loss of Authority Data.
- 13.1.5 The Contractor shall perform secure back-ups of all Authority Data and shall ensure that up-to-date back-ups are stored securely off-site. The Contractor shall ensure that such back-ups are made available to the Authority immediately upon request.
- 13.1.6 The Contractor shall ensure that any system on which the Contractor holds any Authority Data, including back-up data, is a secure system that complies with the Security Policy Framework.
- 13.1.7 If Authority Data is corrupted, lost or sufficiently degraded as a result of the Contractor's Default so as to be unusable, the Authority may:
 - (a) require the Contractor (at the Contractor's expense) to restore or procure the restoration of Authority Data and the Contractor shall do so promptly; and/or
 - (b) itself restore or procure the restoration of Authority Data, and shall be repaid by the Contractor any reasonable expenses incurred in doing so.
- 13.1.8 If at any time the Contractor suspects or has reason to believe that Authority Data has or may become corrupted, lost or sufficiently degraded in any way for any reason, then the Contractor shall notify the Authority immediately and inform the Authority of the remedial action the Contractor proposes to take.

13.2 Personal Data

- 13.2.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller, and the Contractor is the Processor.
- 13.2.2 The Parties agree that they will comply with the provisions on Processing, Personal Data and Data Subjects in Schedule 4.
- 13.2.3 The Parties shall at all times comply with Data Protection Legislation.

13A Security

- 13A.1 The Authority shall be responsible for maintaining the security of the Authority's Premises in accordance with its standard security requirements. The Contractor shall comply with all security requirements of the Authority while on the Authority's Premises and shall ensure that all Staff comply with such requirements.
- 13A.2 The Contractor shall ensure that the Security Plan produced by the Contractor fully complies with Schedule 5 (Security Requirements and Plan).

- 13A.3 The Contractor shall comply, and shall procure compliance of its Staff, with Schedule 5 (Security Requirements and Plan).
- 13A.4 The Authority shall notify the Contractor of any changes or proposed changes to Schedule 5 (Security Requirements and Plan). Any changes shall be agreed in accordance with the procedure in clause 20.3.
- 13A.5 Until and/or unless a change to the Price is agreed by the Authority, the Contractor shall continue to perform the Services in accordance with its existing obligations.
- 13A.6 The Contractor shall be liable for and shall indemnify the Authority against all Losses suffered or incurred by the Authority and/or any third party arising from and/or in connection with any Breach of Security or attempted Breach of Security (to the extent that such Losses were not caused by any act or omission by the Authority).

14 Liability and Insurance

- 14.1 The Contractor shall not be responsible for any injury, loss, damage, cost or expense suffered by the Authority 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 the Contract.
- 14.2 Subject always to clauses 14.3, 14.4 and 14.5:
- 14.2.1 the aggregate liability of the Contractor in respect of all defaults, claims, losses or damages howsoever caused, whether arising from breach of the Contract, the supply or failure to supply of the Services, misrepresentation (whether tortious or statutory), tort (including negligence), breach of statutory duty or otherwise shall in no event exceed a sum equal to 125% of the estimated yearly Price paid or payable to the Contractor under this Contract; and
- 14.2.2 except in the case of claims arising under clauses 9.4 and 18.4 in no event shall the Contractor be liable to the Authority for any:
- a) loss of profits;
 - b) loss of business;
 - c) loss of revenue;
 - d) loss of or damage to goodwill;
 - e) loss of savings (whether anticipated or otherwise); and/or
 - f) any indirect, special or consequential loss or damage.
- 14.3 Nothing in the Contract shall be construed to limit or exclude either Party's liability for:
- 14.3.1 death or personal injury caused by its negligence or that of its Staff;

- 14.3.2 fraud or fraudulent misrepresentation by it or that of its Staff; or
- 14.3.3 any other matter which, by law, may not be excluded or limited.
- 14.4 The Contractor's liability under the indemnity in clauses 9.4 and 18.4 shall be unlimited.
- 14.5 The Contractor's liability for all Losses suffered or incurred by the Authority arising from the Contractor's Default resulting in the destruction, corruption, degradation or damage to Authority Data or Personal Data or any copy of such Authority Data or Personal Data shall in no event exceed £50,000.00.
- 14.6 The Contractor shall hold:
- a) Employer's liability insurance of £5,000,000 providing an adequate level of cover in respect of all risks which may be incurred by the Contractor;
 - b) Public liability with the minimum cover per claim of one million pounds £1,000,000;
 - c) Product liability with the minimum cover per claim of one million pounds £1,000,000;
 - d) Professional indemnity with the minimum cover per claim of one million pounds (£1,000,000);

or any sum as required by Law unless otherwise agreed with the Authority in writing. Such insurance shall be maintained for the duration of the Term and for a minimum of six (6) years following the expiration (or 12 (Twelve) years if the Contract is executed as a deed) or earlier termination of the Contract.

15 Force Majeure

- 15.1 Neither Party shall have any liability under or be deemed to be in breach of the Contract for any delays or failures in performance of the Contract which result from circumstances beyond the reasonable control of the Contractor. Each Party shall promptly notify the other Party in writing, using the most expeditious method of delivery, when such circumstances cause a delay or failure in performance, an estimate of the length of time delay or failure shall continue and when such circumstances cease to cause delay or failure in performance. If such circumstances continue for a continuous period of more than 30 days, either Party may terminate the Contract by written notice to the other Party.
- 15.2 Any failure by the Contractor in performing its obligations under the Contract which results from any failure or delay by an agent, sub-contractor or Contractor shall be regarded as due to Force Majeure only if that agent, sub-contractor or Contractor is itself impeded by Force Majeure from complying with an obligation to the Contractor.

16 Termination

- 16.1 The Authority may terminate the Contract at any time by notice in writing to the Contractor to take effect on any date falling at least 1 month (or, if the Contract is less than 3 months in duration, at least 10 Working Days) later than the date of service of the relevant notice.
- 16.2 Without prejudice to any other right or remedy it might have, the Authority may terminate the Contract by written notice to the Contractor with immediate effect if the Contractor:
 - 16.2.1 (without prejudice to clause 16.2.5), is in material breach of any obligation under the Contract which is not capable of remedy;
 - 16.2.2 repeatedly breaches any of the terms and conditions of the Contract in such a manner as to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms and conditions of the Contract;
 - 16.2.3 is in material breach of any obligation which is capable of remedy, and that breach is not remedied within 30 days of the Contractor receiving notice specifying the breach and requiring it to be remedied;
 - 16.2.4 undergoes a change of control within the meaning of section 416 of the Income and Corporation Taxes Act 1988;
 - 16.2.5 breaches any of the provisions of clauses 7.2, 11, 12, 13, 17, 18.4 and 20.11; or
 - 16.2.6 becomes insolvent, or if an order is made or a resolution is passed for the winding up of the Contractor (other than voluntarily for the purpose of solvent amalgamation or reconstruction), or if an administrator or administrative receiver is appointed in respect of the whole or any part of the Contractor's assets or business, or if the Contractor makes any composition with its creditors or takes or suffers any similar or analogous action (to any of the actions detailed in this clause 16.2.6) in consequence of debt in any jurisdiction.
- 16.3 The Contractor shall notify the Authority as soon as practicable of any change of control as referred to in clause 16.2.4 or any potential such change of control.
- 16.4 The Contractor may terminate the Contract by written notice to the Authority if the Authority has not paid any undisputed amounts within 90 days of them falling due.
- 16.5 If the Authority terminates the Contract under this clause, the Authority shall make no further payments to the Contractor except for Services supplied by the Contractor prior to termination and in accordance with the Contract but where the payment has yet to be made by the Authority.
- 16.6 Termination or expiry of the Contract shall be without prejudice to the rights of either Party accrued prior to termination or expiry and shall not affect the continuing rights

of the Parties under this clause and clauses 2, 3.2, 6.1, 6.2, 6.6, 6.7, 7, 9, 10.2, 11, 12, 13, 13A, 14, 16.8, 17.4, 18.4, 19 and 20.8 or any other provision of the Contract that either expressly or by implication has effect after termination.

16.7 Termination by Convenience:

16.7.1 The Authority shall have the right to terminate the Contract any time for any reason by giving no less than 4 weeks prior written notice.

16.7.2 The Contractor shall have the right to terminate the Contract any time for any reason by giving no less than 4 weeks prior written notice.

16.8 Upon termination or expiry of the Contract, the Contractor shall:

16.8.1 give all reasonable assistance to the Authority and any incoming Contractor of the Services to the extent necessary to effect an orderly assumption by a Replacement Contractor in accordance with the procedure set out in Schedule 8 – Exit Management Strategy; and

16.8.2 return all requested documents, information and data to the Authority as soon as reasonably practicable.

17 Compliance

17.1 The Contractor shall promptly notify the Authority of any health and safety hazards which may arise in connection with the performance of its obligations under the Contract. The Authority shall promptly notify the Contractor of any health and safety hazards which may exist or arise at the Authority's premises and which may affect the Contractor in the performance of its obligations under the Contract.

17.2 The Contractor shall:

17.2.1 comply with all the Authority's health and safety measures while on the Authority's premises; and

17.2.2 notify the Authority immediately of any incident occurring in the performance of its obligations under the Contract on the Authority's premises where that incident causes any personal injury or damage to property which could give rise to personal injury.

17.3 The Contractor shall:

17.3.1 perform its obligations under the Contract in accordance with all applicable equality Law and the Authority's equality and diversity policy as provided to the Contractor from time to time; and

17.3.2 take all reasonable steps to secure the observance of clause 17.3.1 by all Staff.

- 17.4 The Contractor shall supply the Services in accordance with the Authority's environmental policy as provided to the Contractor from time to time.
- 17.5 The Contractor shall comply with, and shall ensure that its Staff shall comply with, the provisions of:
 - 17.5.1 the Official Secrets Acts 1911 to 1989; and
 - 17.5.2 section 182 of the Finance Act 1989.

18 Prevention of Fraud, Corruption and Bribery

- 18.1 The Contractor represents and warrants that neither it, nor to the best of its knowledge any Staff, have at any time prior to the Commencement Date:
 - 18.1.1 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
 - 18.1.2 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.
- 18.2 The Contractor shall not during the Term:
 - 18.2.1 commit a Prohibited Act; and/or
 - 18.2.2 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.
- 18.3 The Contractor shall, during the Term 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; and shall notify the Authority immediately if it has reason to suspect that any breach of clauses 18.1 and/or 18.2 has occurred or is occurring or is likely to occur.
- 18.4 If the Contractor or the Staff engages in conduct prohibited by clause 18.1 or commits fraud in relation to the Contract or any other contract with the Crown (including the Authority) the Authority may:
 - 18.4.1 terminate the Contract and recover from the Contractor the amount of any loss suffered by the Authority resulting from the termination, including the cost reasonably incurred by the Authority of making other arrangements for the supply of the Services and any additional expenditure incurred by the Authority throughout the remainder of the Contract; or

- 18.4.2 recover in full from the Contractor any other loss sustained by the Authority in consequence of any breach of this clause.

19 Dispute Resolution

- 19.1 The Parties shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with the 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 an appropriately senior representative of each Party.
- 19.2 If the dispute cannot be resolved by the Parties within one month of being escalated as referred to in clause 19.1, the dispute may by agreement between the Parties be referred to a neutral adviser or mediator (the “Mediator”) chosen by agreement between the Parties. All negotiations connected with the dispute shall be conducted in confidence and without prejudice to the rights of the Parties in any further proceedings.
- 19.3 If the Parties fail to appoint a Mediator within one month 20 Working Days of the agreement to refer to a Mediator, either Party shall apply to the Centre for Effective Dispute Resolution to appoint a Mediator.
- 19.4 If the Parties fail to enter into a written agreement resolving the dispute within one month of the Mediator being appointed, or such longer period as may be agreed by the Parties, either Party may refer the dispute to Court.
- 19.5 The commencement of mediation shall not prevent the parties commencing or continuing court or arbitration proceedings in relation to the dispute.

20 General

- 20.1 Each of the Parties represents and warrants to the other that it has full capacity and authority, and all necessary consents, licences and permissions to enter into and perform its obligations under the Contract, and that the Contract is executed by its duly authorised representative.
- 20.2 A person who is not a party to the Agreement shall have no right to enforce any of its provisions which, expressly or by implication, confer a benefit on him, without the prior written agreement of the Parties. This clause does not affect any right or remedy of any person which exists or is available apart from the Contracts (Rights of Third Parties) Act 1999 and does not apply to the Crown.
- 20.3 Subject to Clause 3.4, the Contract cannot be varied except in writing signed by a duly authorised representative of both the Parties.
- 20.4 In the event that the Contractor is unable to accept the Variation to the Specification or where the Parties are unable to agree a change to the Contract Price, the Authority may:
- 20.4.1 allow the Contractor to fulfil its obligations under the Contract without the Variation to the Specification;

- 20.4.2 terminate the Contract with immediate effect, except where the Contractor has already provided all or part of the Services or where the Contractor can show evidence of substantial work being carried out to fulfil the requirement of the Specification, and in such case the Parties shall attempt to agree upon a resolution to the matter. Where a resolution cannot be reached, the matter shall be dealt with under the Dispute Resolution procedure detailed at clause 19.
- 20.5 The Contract contains the whole agreement between the Parties and supersedes and replaces any prior written or oral agreements, representations or understandings between them. The Parties confirm that they have not entered into the Contract on the basis of any representation that is not expressly incorporated into the Contract. Nothing in this clause shall exclude liability for fraud or fraudulent misrepresentation.
- 20.6 Any waiver or relaxation either partly, or wholly of any of the terms and conditions of the Contract shall be valid only if it is communicated to the other Party in writing and expressly stated to be a waiver. A waiver of any right or remedy arising from a breach of contract shall not constitute a waiver of any right or remedy arising from any other breach of the Contract.
- 20.7 The Contract shall not constitute or imply any partnership, joint venture, agency, fiduciary relationship or other relationship between the Parties other than the contractual relationship expressly provided for in the Contract. Neither Party shall have, nor represent that it has, any authority to make any commitments on the other Party's behalf.
- 20.8 Except as otherwise expressly provided by the Contract, all remedies available to either Party for breach of the Contract (whether under the Contract, statute or common law) are cumulative and may be exercised concurrently or separately, and the exercise of one remedy shall not be deemed an election of such remedy to the exclusion of other remedies.
- 20.9 If any provision of the Contract is prohibited by law or judged by a court to be unlawful, void or unenforceable, the provision shall, to the extent required, be severed from the Contract and rendered ineffective as far as possible without modifying the remaining provisions of the Contract, and shall not in any way affect any other circumstances of or the validity or enforcement of the Contract.
- 20.10 The Contractor shall take appropriate steps to ensure that neither the Contractor 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 Contractor and the duties owed to the Authority under the provisions of the Contract. The Contractor will disclose to the Authority full particulars of any such conflict of interest which may arise.
- 20.11 The Authority reserves the right to terminate the Contract immediately by notice in writing and/or to take such other steps it deems necessary where, in the reasonable opinion of the Authority, there is or may be an actual conflict, or potential conflict between the pecuniary or personal interest of the Contractor and the duties owed to

the Authority pursuant to this clause shall not prejudice or affect any right of action or remedy which shall have accrued or shall thereafter accrue to the Authority.

- 20.12 The Contract constitutes the entire contract between the Parties in respect of the matters dealt with therein. 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 Fraud or fraudulent misrepresentation.

21 Notices

- 21.1 Except as otherwise expressly provided in the Contract, no notice or other communication from one Party to the other shall have any validity under the Contract unless made in writing by or on behalf of the Party concerned.

- 21.2 Any notice or other communication which is to be given by either Party to the other shall be given by letter (sent by hand, first class post, recorded delivery or special delivery), or by facsimile transmission or electronic mail (confirmed in either case by letter). Such letters shall be addressed to the other Party in the manner referred to in clause 21.3. Provided the relevant communication is not returned as undelivered, the notice or communication shall be deemed to have been given 2 Working Days after the day on which the letter was posted, or 4 hours, in the case of electronic mail or facsimile transmission or sooner where the other Party acknowledges receipt of such letters, facsimile transmission or item of electronic mail.

- 21.3 For the purposes of clause 21.2, the address of each Party shall be:

- 21.3.1 For the Authority: Care Quality Commission – on behalf of The Maternity and Newborn Safety Investigations (MNSI)

Address: Citygate, Gallowgate,

Newcastle upon Tyne, NE1 4PA

For the attention of: [REDACTED]

Email: [REDACTED]

- 21.3.2 For the Contractor: Mission Diverse Consulting Ltd

Address: 12 Pheonix Business Park,

Onyx House, Birmingham, B7 4NU

For the attention of: [REDACTED]

Tel: [REDACTED]

Email: [REDACTED]

21.4 Either Party may change its address for service by serving a notice in accordance with this clause.

21.5 Notices under clauses 15 (Force Majeure) and 16 (Termination) may be served by email only if the original notice is then sent to the recipient by personal delivery or recorded delivery in the manner set out in clause 21.1.

22 Governing Law and Jurisdiction

22.1 The validity, construction and performance of the Contract, and all contractual and non-contractual matters arising out of it, shall be governed by English law and shall be subject to the exclusive jurisdiction of the English courts to which the Parties submit.

23 TUPE

Not applicable

IN WITNESS of which this Contract has been duly executed by the parties.

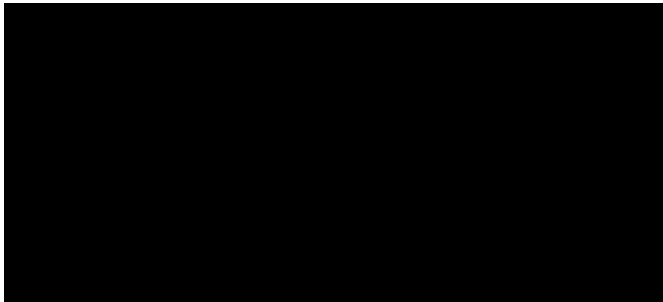
SIGNED for and on behalf of **CARE QUALITY COMMISSION**

Authorised Signatory:

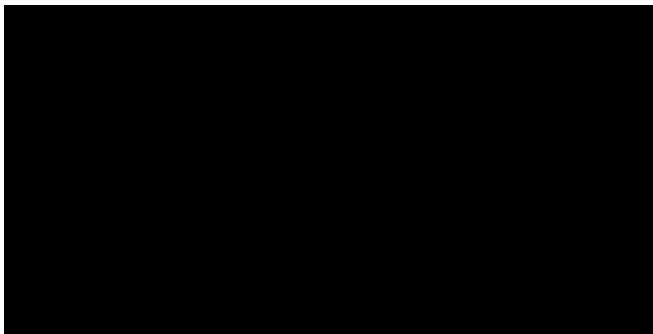


SIGNED for and on behalf of **MISSION DIVERSE CONSULTING LTD**

Authorised Signatory 1:



Authorised Signatory 2:



SCHEDULE 1 –SPECIFICATION

Executive Summary

The Maternity and Newborn Safety Investigations (MNSI) programme is part of a national strategy to improve maternity safety across the NHS in England.

All NHS trusts are required to tell us about certain patient safety incidents that happen in maternity care. This is so that we can carry out an independent investigation and where relevant, make safety recommendations to improve services at local level and across the whole maternity healthcare system in England.

The programme was established in 2018 as part of the Healthcare Safety Investigation Branch and is now hosted by the Care Quality Commission.

Our workforce is made up of approximately 190 team members who undertake, advise and support maternity investigations. The whole team are remote workers with the investigation team members allocated to a dedicated team with associated NHS trusts.

The programme's initial diagnostic work around anti-racism has revealed a significant impact of racism on our Black and Brown colleagues, highlighting the need for a deeper understanding of racism for individuals and across the wider team. Addressing this is crucial to fostering a more inclusive working environment within our team, supporting open and informed conversations and ensuring that our commitment to anti-racism is demonstrated in the work we undertake with families and NHS staff.

MNSI is looking to procure a programme of work that undertakes a variety of approaches to explore, understand and educate the team in relation to racism and the wider inequality agenda.

Whilst we have prioritised the tackling of racism; these actions will foster the development of inclusive behaviours to support all minoritized groups within MNSI, and the families and trust staff we work alongside.

1. The Requirement

This work needs to strengthen and inform MNSI's anti-racism approach to:

- Equip leaders and line managers with a clear understanding of their responsibility to actively address and combat racism and wider inequalities.
- Engage the wider team in deepening both individual and collective understanding of anti-racism.
- Ensure anti-racism becomes a deeply embedded and sustained practice in every aspect of our work.
- Foster an environment that encourages open dialogue and exploration of racism, wider inequalities and their impact.
- Prioritise psychological safety to create a space where team members feel secure in

discussing and addressing racism and wider inequalities.

How would this be done:

- This needs to be done through a variety of approaches to access the whole team. These may include:
 - Focus groups
 - Face to face training
 - Some e-learning to reinforce the messaging
 - Specific training for line managers
 - Assessment of understanding

Other approaches may be needed to support the specific needs of individuals.

2. Cost Envelope

Cost Envelope
£160,000 to £180,000 Including VAT for the initial 2 years

3. Duration of Contract

Start Date	End Date	Extension Options (If Applicable)
14/04/2025	31/03/2027	Up to 12-month extension

4. Authority Responsibilities

CQC responsibilities

The Authority will ensure all milestone payments are made promptly in line with the contract.

5. Supplier Responsibilities

The supplier shall:

- Appoint a contract and/or a programme manager to oversee the work and liaise with/report as required to MNSI/CQC's programme manager.
- Agree the nature and frequency of meetings required with MNSI/CQC.
- Perform quality assurance on all aspects of the programme.
- Provide MNSI/CQC with timely and ongoing evaluation and quality assurance information relating to the programme.
- Provide MNSI/CQC with updates on costs and progress as required.

6. Contract Management Arrangements

There will be a clear programme plan with deliverables which will be monitored by CQC and the supplier.

Additionally, the supplier will be expected to:

- Communicate and meet (e.g. online) frequently with MNSI/CQC as agreed
- Work within agreed key performance indicators relating to quality, delivery of products and levels of service
- Measure performance and provision of service on an ongoing basis against specific target dates
- Provide reports on progress to the contract manager / programme manager
- Attend key meetings in person to review progress and discuss the service, as required by the contract manager / programme manager
- Attend a post contract review with the MNSI/CQC to review whether the objectives of the contract were met, to review the benefits achieved
- Identify any lessons learnt for future programmes.

7. Key Performance Indicators (KPIs)

Indicator	Measured by	Target	Review Frequency
Resource mobilisation in line with requirements	The successful supplier is required to ensure that personnel and	100% of services to be delivered as agreed	Monthly

	other resources to deliver the service as agreed in the cost breakdown will be in place to ensure delivery on time and to the quality standards required.		
Focus groups – delegate evaluation	Evaluation surveys or other agreed method of gathering participant feedback	75% participants	After each focus group and part of supplier reports
Face to face training – delegate evaluation	Evaluation surveys or other agreed method of gathering participant feedback	75% participants	After each training session and part of supplier reports
Participant accessibility requirements for any eLearning	Participant and supplier feedback	75% of respondents feedback on accessibility needs	As part of supplier reports

8. Milestones

The table below sets out a proposed timetable of activity. Please note that this is intended as a guide and is subject to change to ensure the greatest alignment with our transformational change programme. We will work with the successful supplier upon commencement of the contract to agree the programme for delivery.

Description	Target Date	Action to Achieve Milestone	Review Date
Scoping	Month 1	Delivery of structured plan	End of April 2025
Line managers focus group	Month 2	Confirmation all line managers have completed and feedback	End of May 2025
Remaining team focus groups	Months 3-4	Confirmation all staff members have completed and feedback	End of August 2025 – this will need consideration around A/L
Review of priority areas of focus	Months 4-5	Structured delivery plan from focus groups	Aug/Sept
Delivery of areas of priority	Months 6-12	Structured delivery plan of focused areas	Sept – Feb 2026
Review and evaluation of impact to inform Y2	Month 12	Evaluation of Y1 and evidence of change	Feb /March 2026

9. Skills and Knowledge Transfer

Participants will be able to: -

- Reflect on their own behaviours and values.
- Have a deeper understanding of anti-racism

SCHEDULE 2 – CONTRACTOR’S RESPONSE

Evaluation Criteria 1: Delivery approach and Methodology

Describe how you intend to deliver our requirements as stated in Appendix A: Statement of Requirements

Your response should include but not be limited to:

- Demonstrating how you will engage the wider team in deepening both individual and collective understanding of anti-racism.
- Demonstrating how you will prioritise psychological safety to create a space where team members feel secure in discussing and addressing racism and wider inequalities.
- Demonstrating how you will foster an environment that encourages open dialogue and exploration of racism, wider inequalities and their impact.
- Demonstrating how you will equip leaders and line managers with a clear understanding of their responsibility to actively address and combat racism and wider inequalities.

Supporting Attachment Required? Yes

Appendix A_Relevant Staff Experience

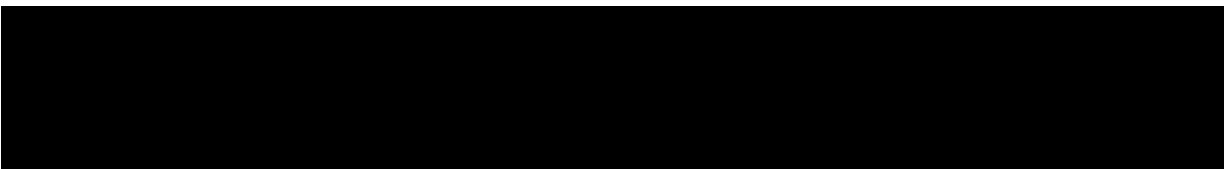
Appendix E_Proposed Course Learning Outline

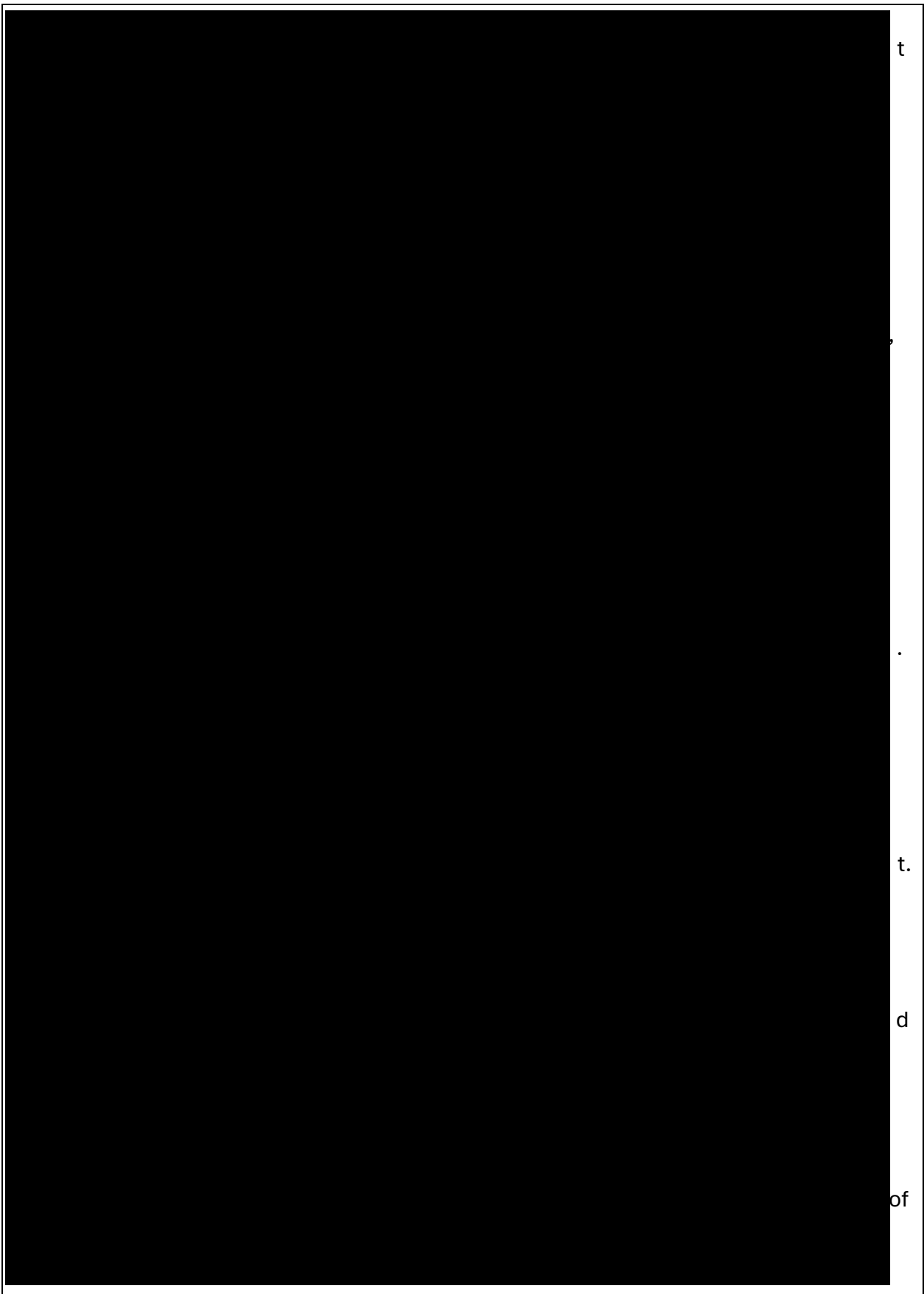
Scoring mechanism: 0 – 4 as per ITT Table 5

Weighting/Max Score: 20%

Max Word Count: 1500

Evaluation Criteria 1 Bidder Response.





t

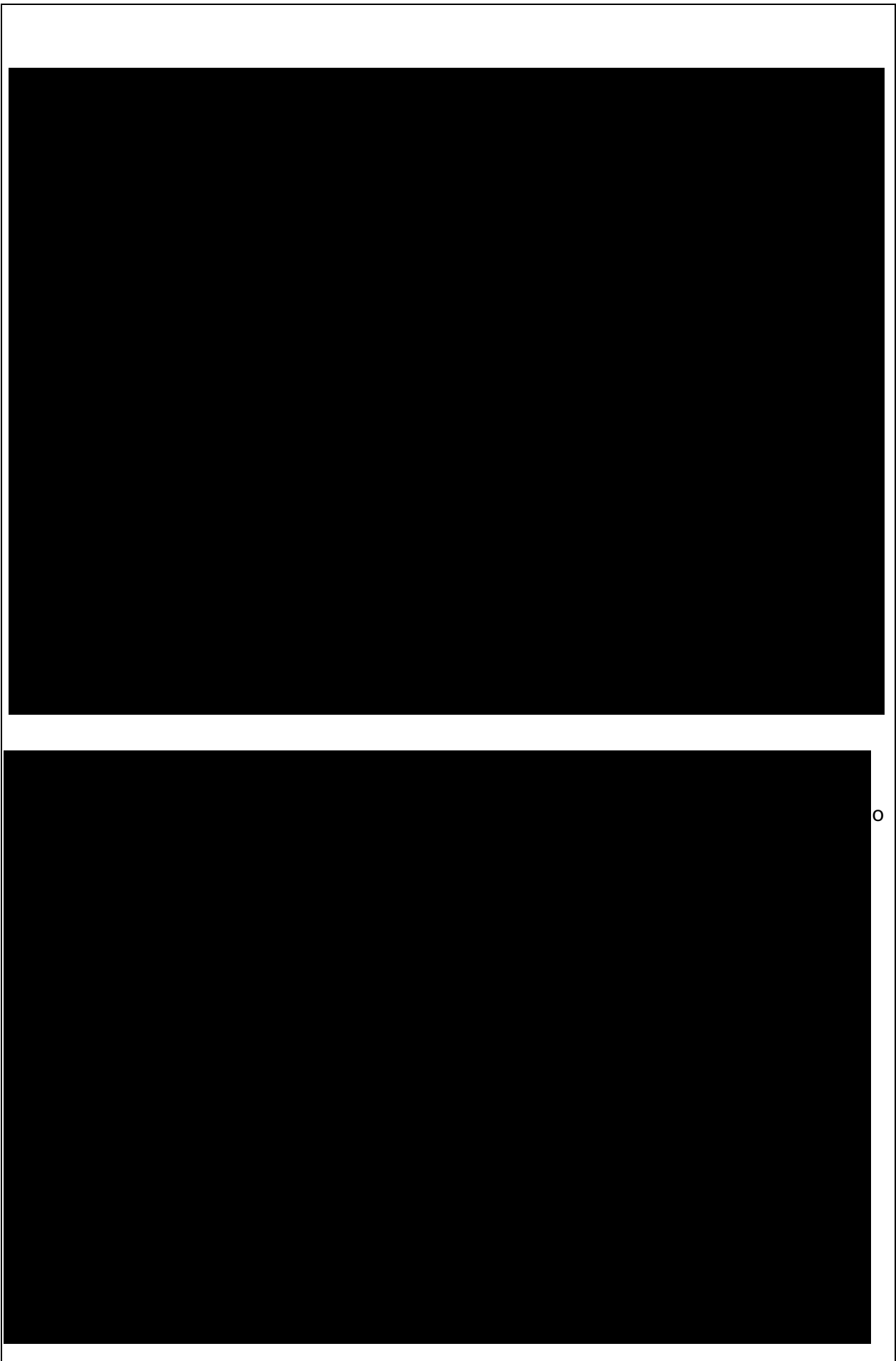
.

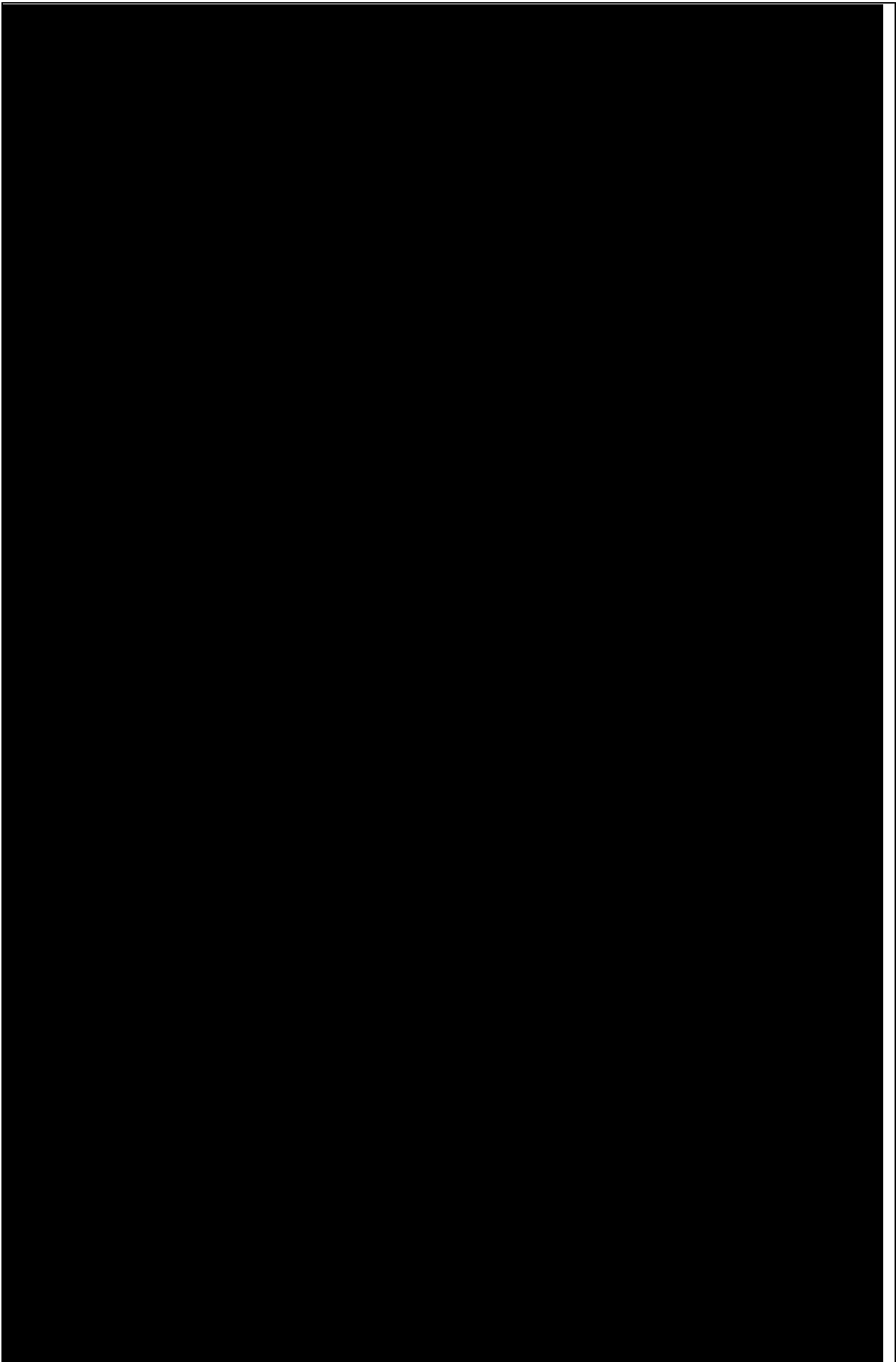
.

t.

d

of





[REDACTED]

[REDACTED]

[546-](#)

[REDACTED]

t

Evaluation Criteria 2: Monitoring and Quality Assurance

Describe your approach to monitoring and quality assurance of our requirements as stated in Appendix A: Statement of Requirements.

Your response should address the following:

- Demonstrate how you will measure the impact and effectiveness of each milestone
- Demonstrate how you will monitor and ensure an inclusive learning experience for all participants and quality assurance will be delivered
- Demonstrate how you will ensure learning retention and sustainability
- Demonstrate how you will monitor and resolve complaints and issues
- Provide up to two examples of your reporting processes, including details of team progress and development
- Evidence resilience in the event of training or a planned event cannot be facilitated

Supporting Attachment Required? Yes

Appendix B_Learner Engagement and Retention Model

Scoring mechanism: 0 – 4 as per ITT Table 5

Weighting/Max Score: 20%

Max Word Count: 1500

[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]

[Redacted content]

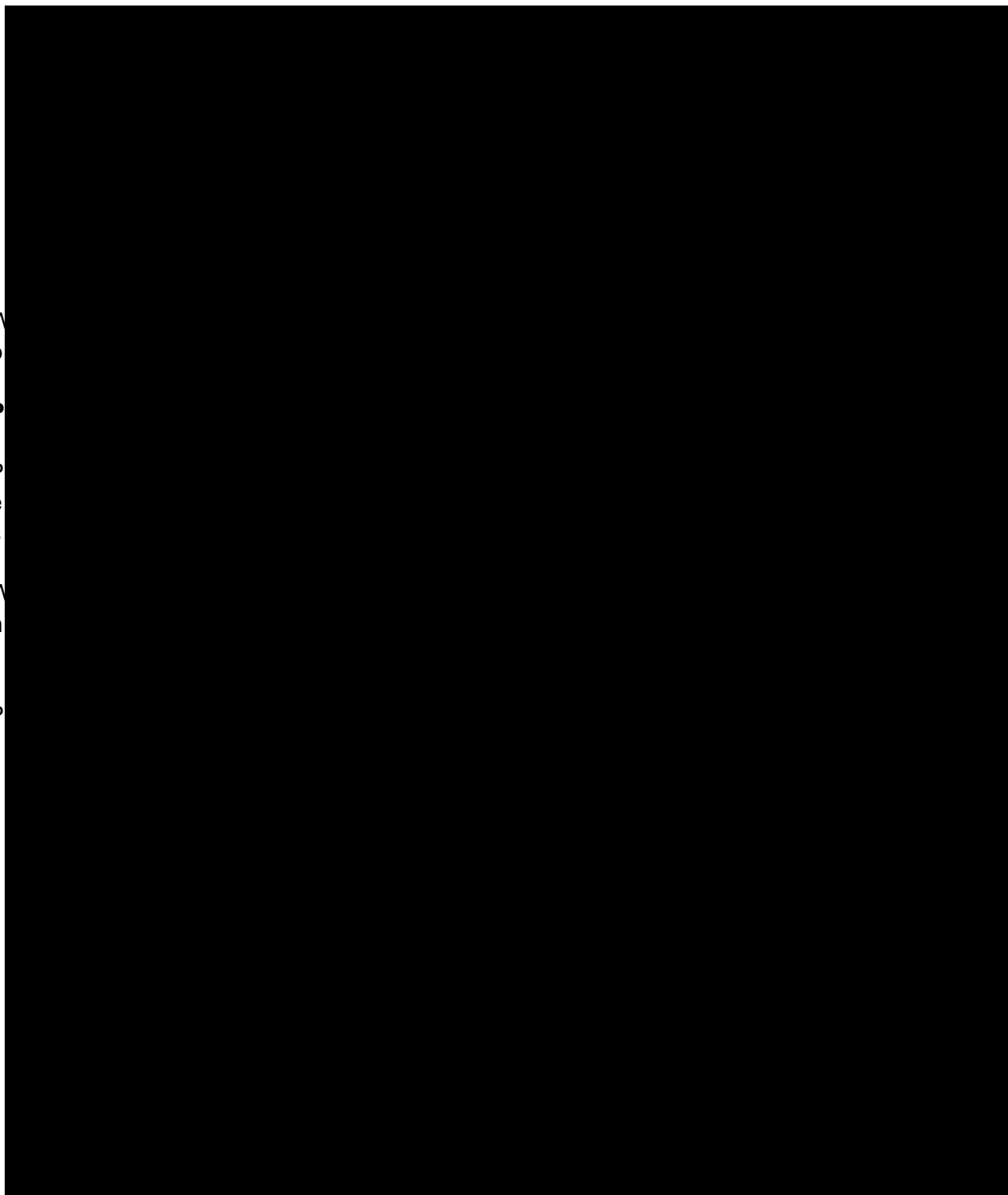
[Redacted content]

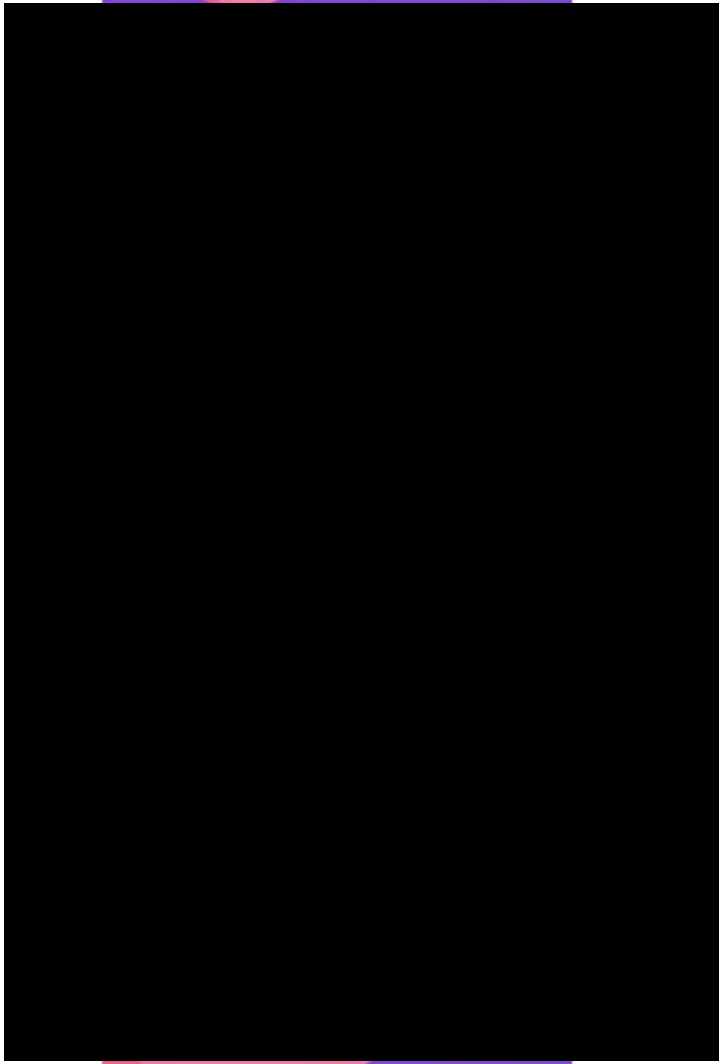
[Redacted content]

[Redacted content]

[Redacted content]

•
•
I
W
o
P
P
e
s
W
h
r
P
r

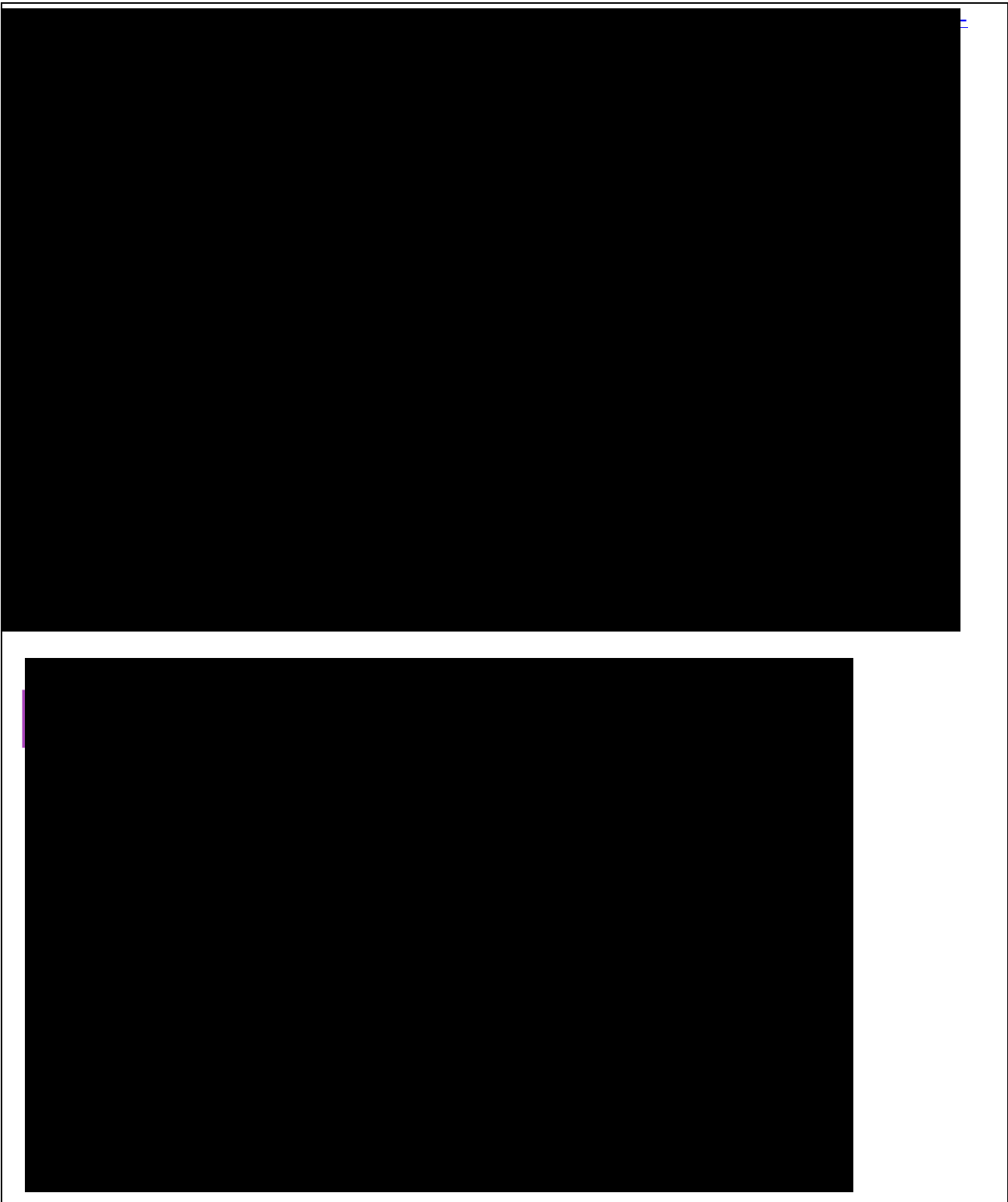


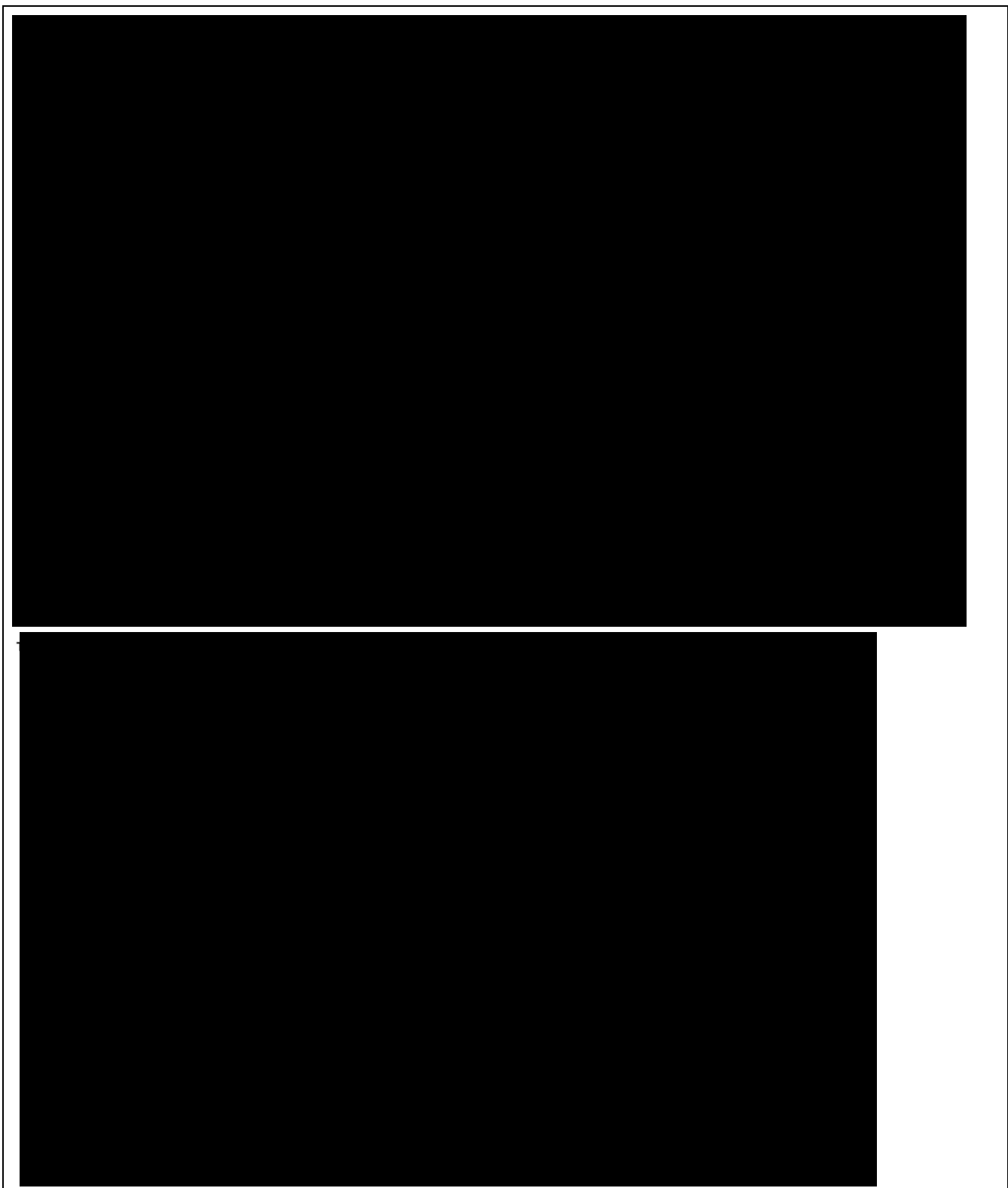


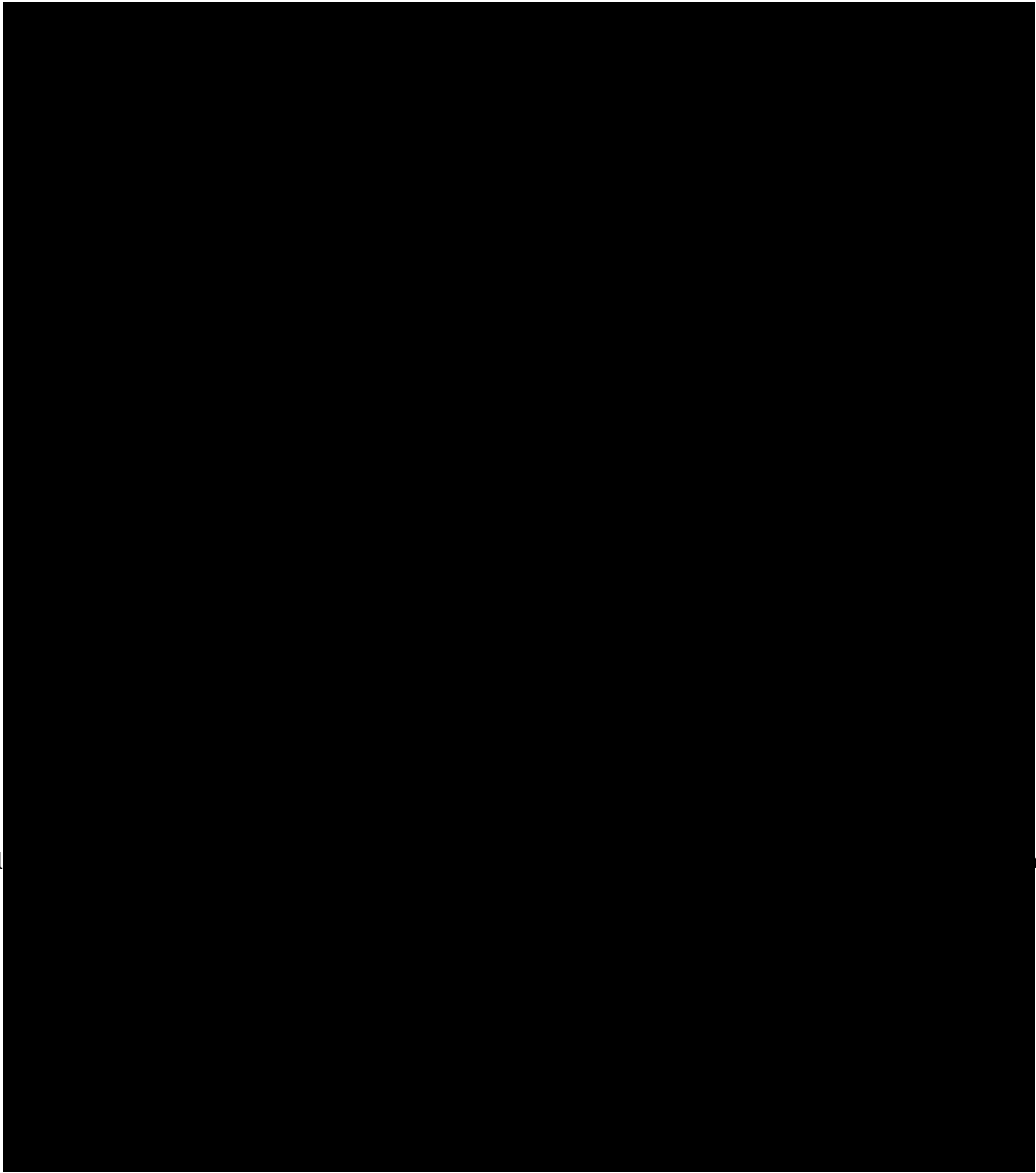
MISSION
DIVERSE

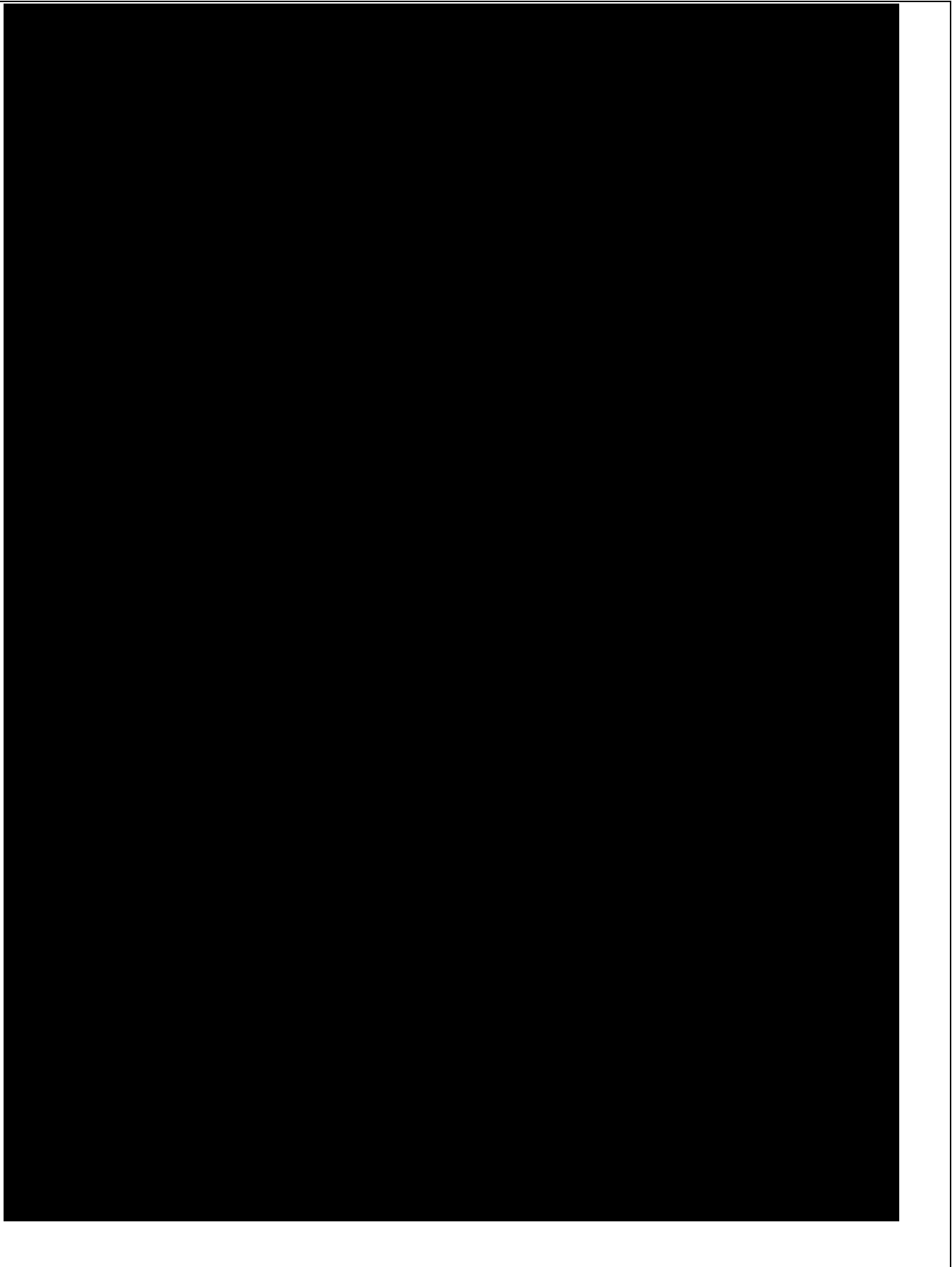


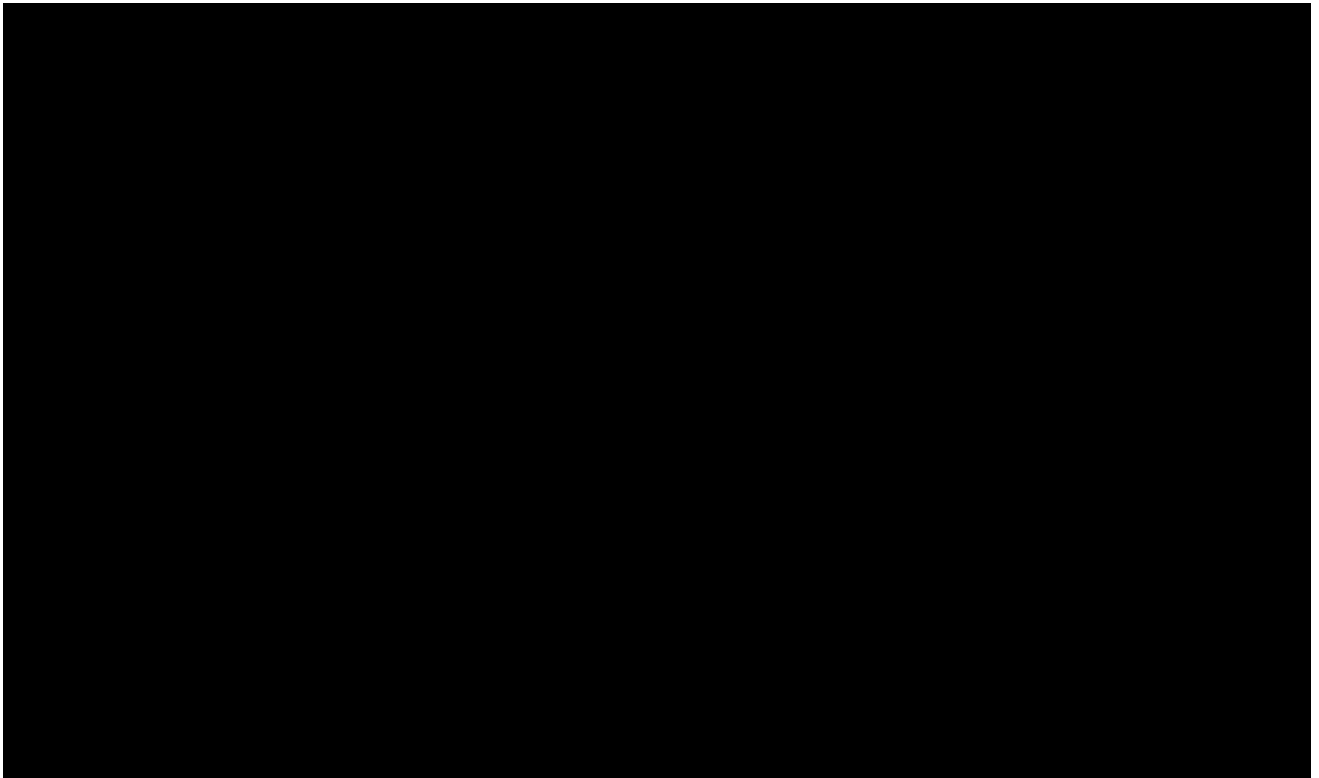
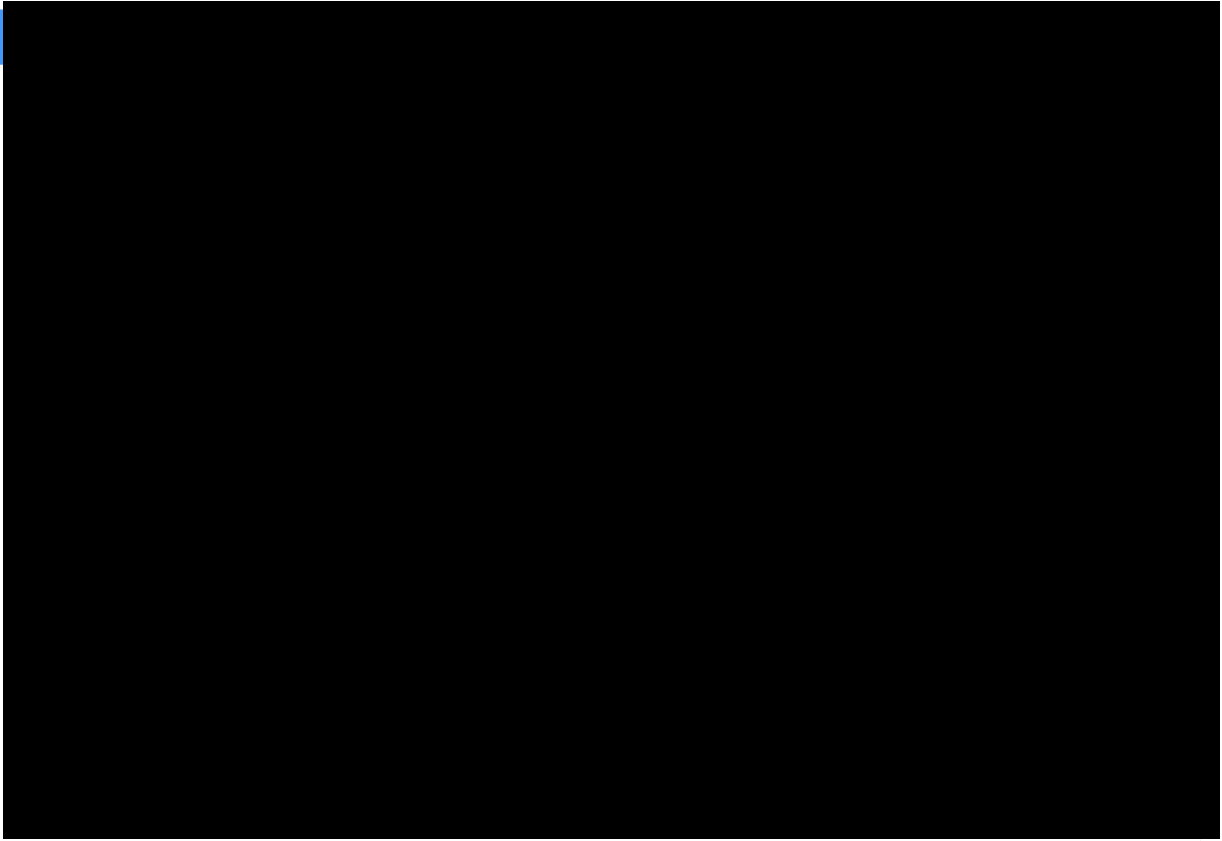
[Redacted text]

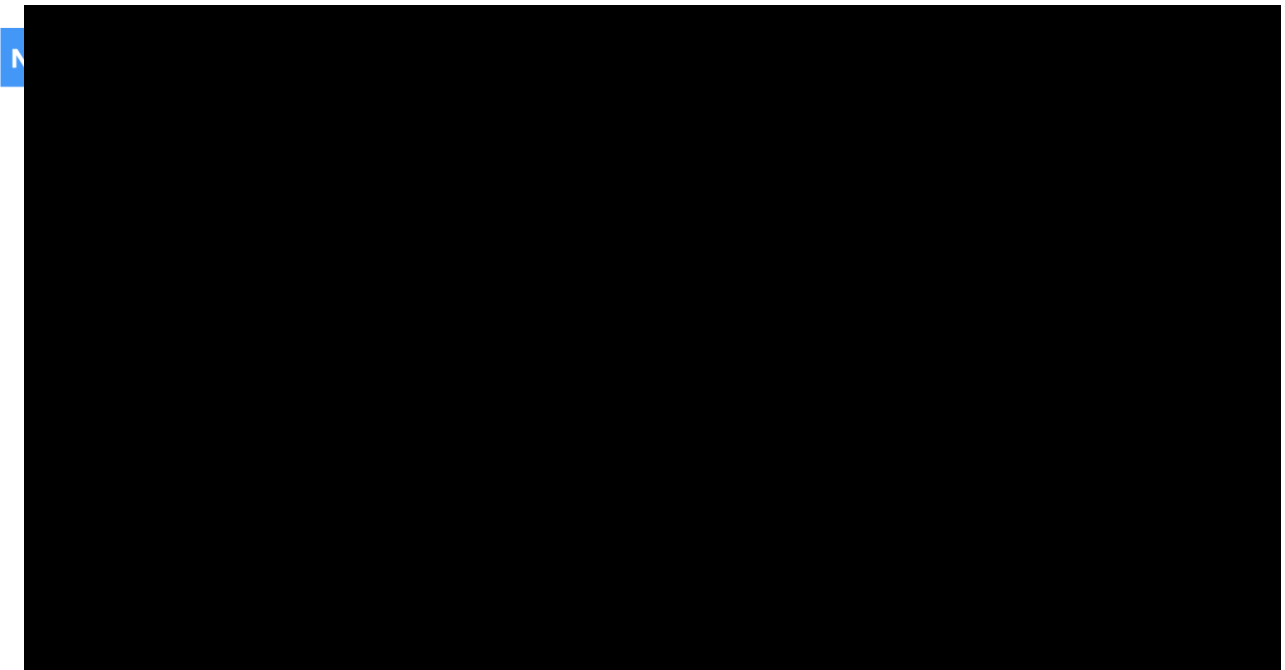
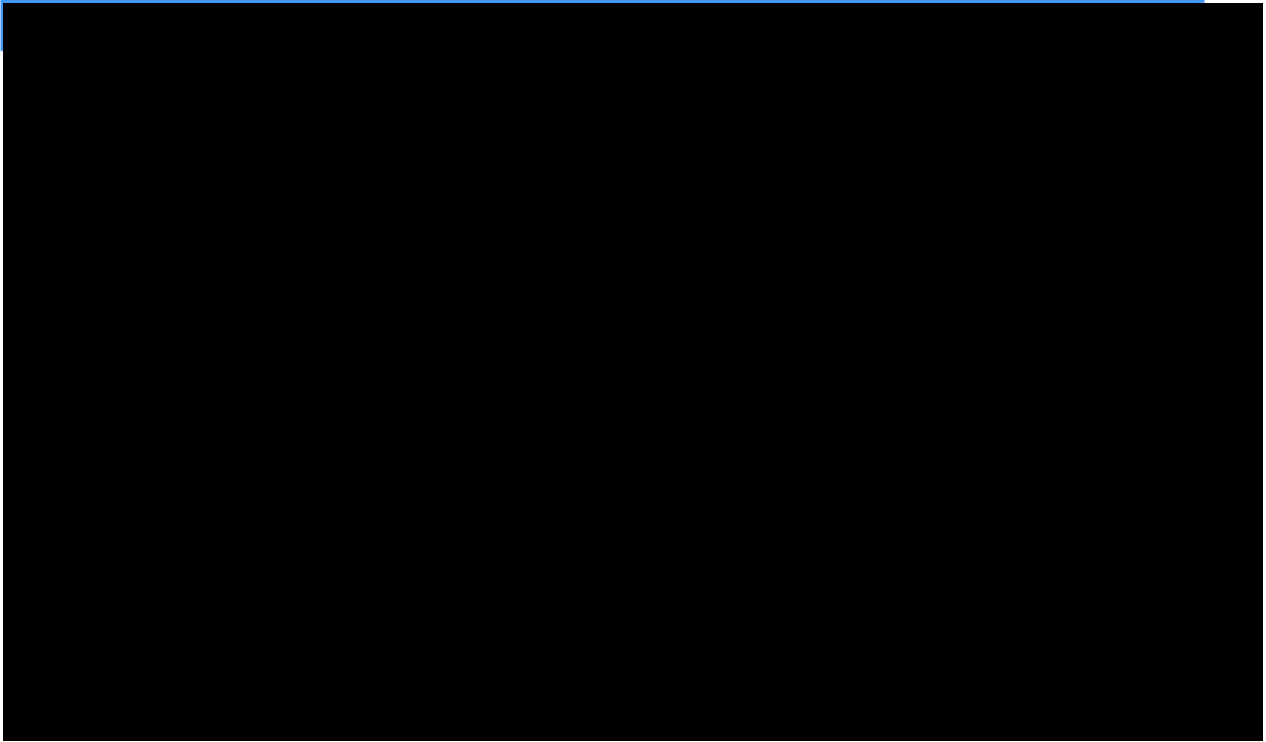


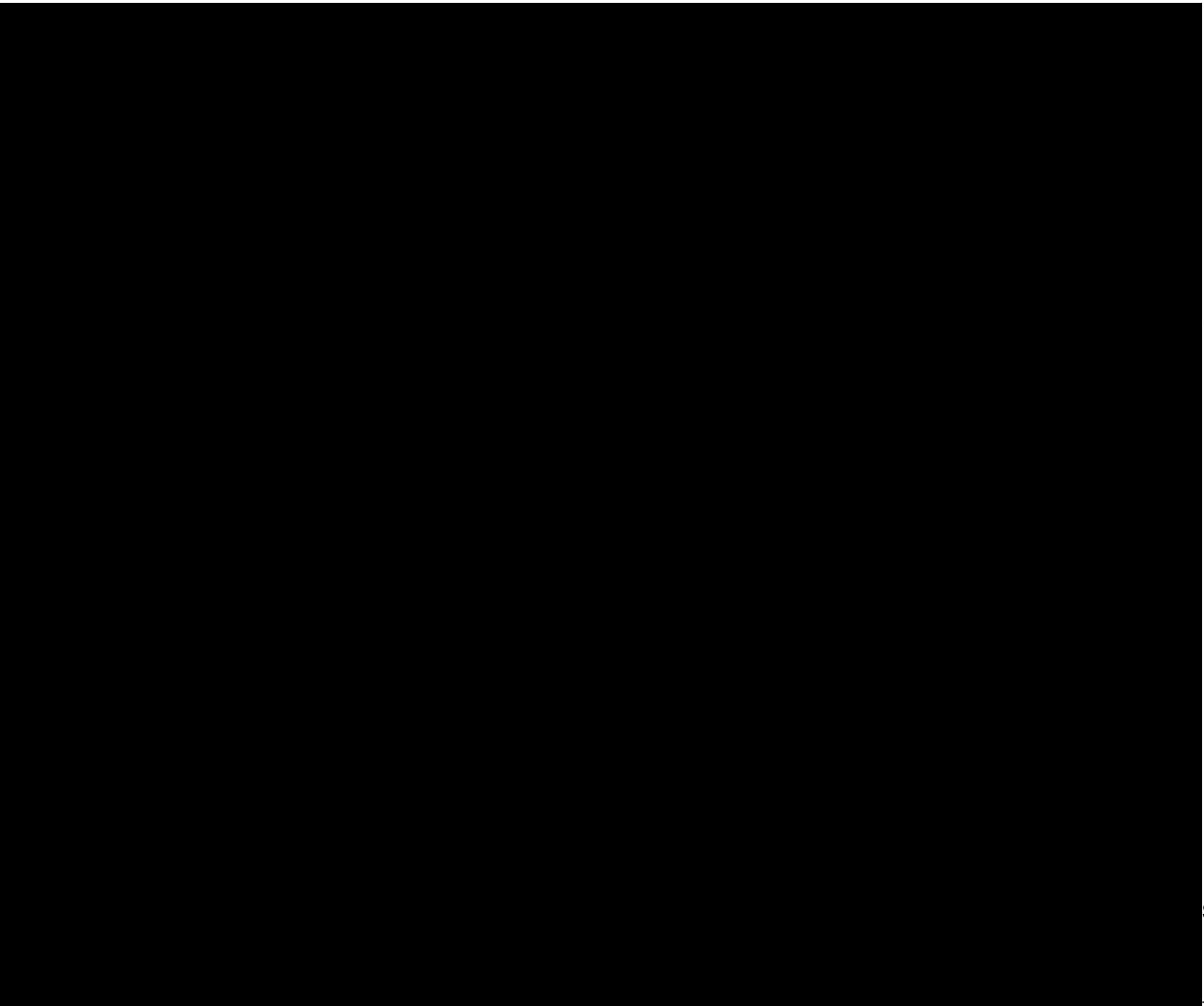
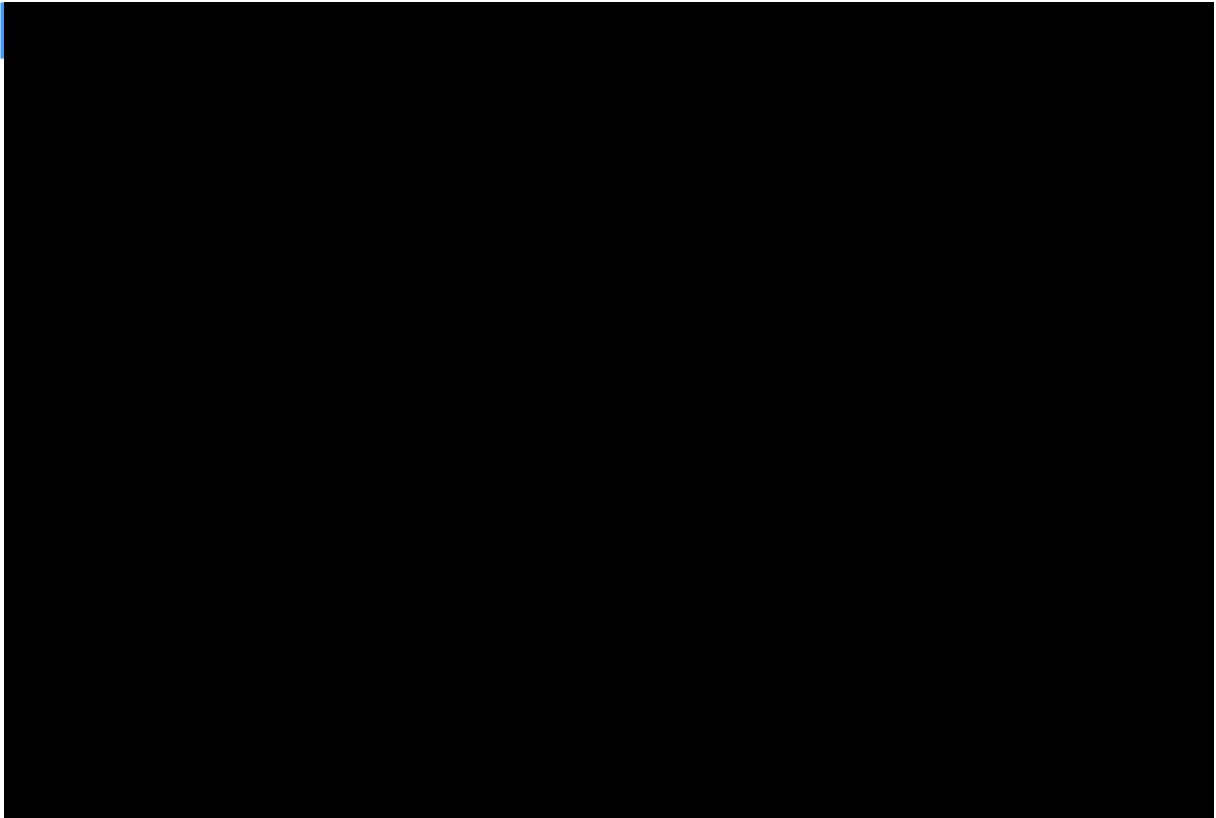












a

d

g

s,

[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]

- [REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

- [REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED]
[REDACTED]

business days.

[REDACTED]

- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

-
- | Response | Percentage |
|--|------------|
| Yes, the U.S. should take action to reduce greenhouse gas emissions | 85% |
| No, the U.S. should not take action to reduce greenhouse gas emissions | 15% |

_____ u _____

[REDACTED]

[illegible]

Scoring mechanism: 0 – 4 as per ITT Table 5

Weighting/Max Score: 20%

Max Word Count: 1500

[REDACTED]

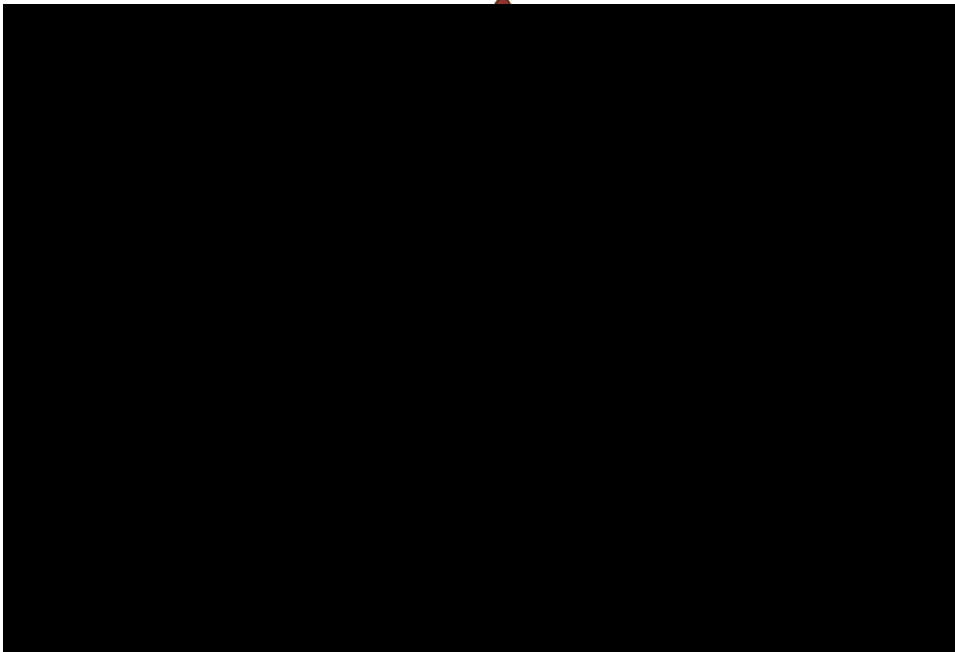
[REDACTED]

[REDACTED]

[REDACTED]

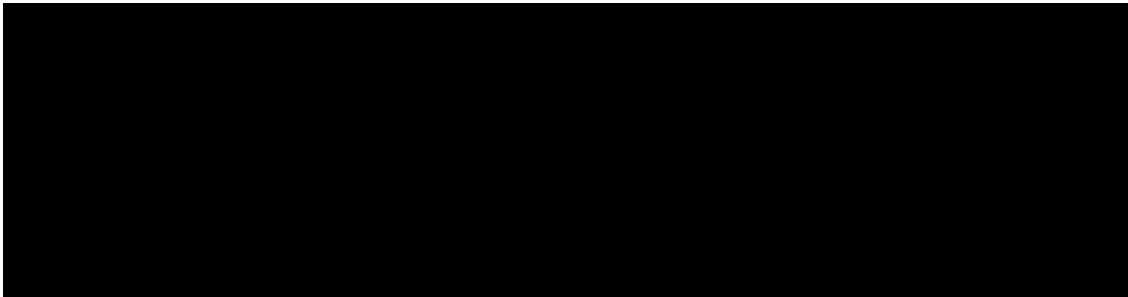
■ [REDACTED]ses and

■ [REDACTED]



5. Critical Thinking

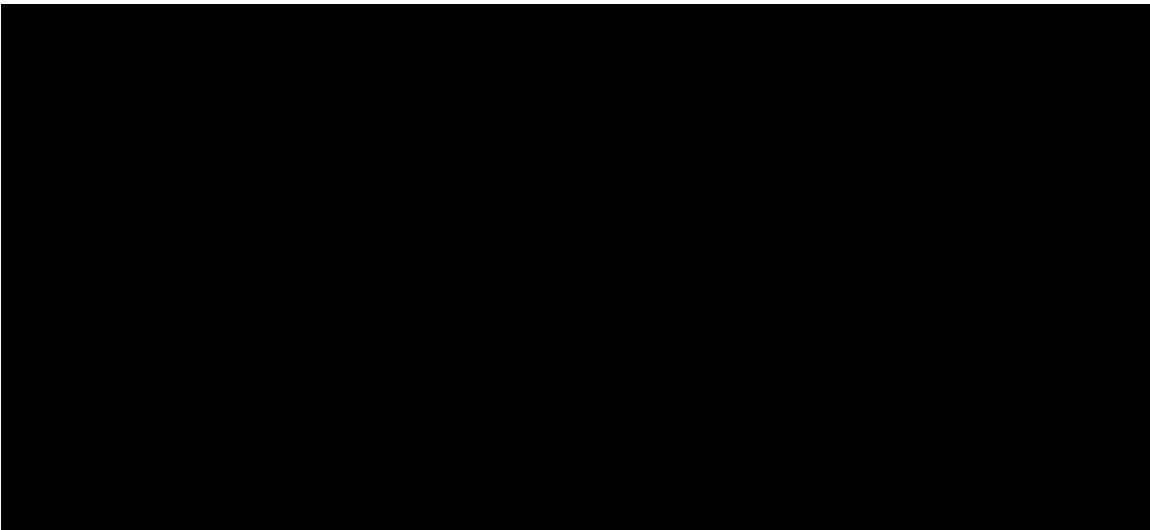
-



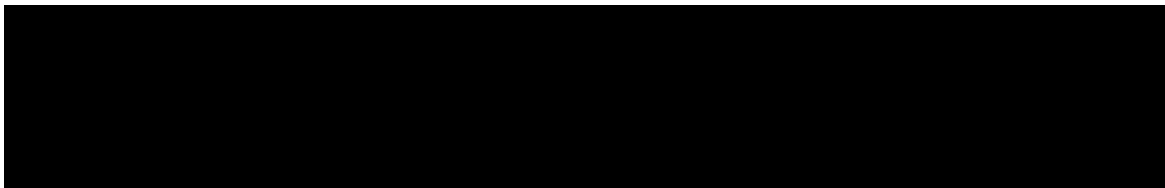
-

-

B
e



es,



[illegible]

C

I

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

[REDACTED]

[REDACTED]

Evaluation Criteria 4: Accessibility and Inclusion

Describe how you will ensure all the services and contents are fully accessible, so everyone can access learning, including people with disabilities and neurodiversity requirements.

Supporting Attachment Required? Yes

Appendix D_Mission Diverse Accessibility Statement

Scoring mechanism: 0 – 4 as per ITT Table 5

Weighting/Max Score: 10%

Max Word Count: 1000

E

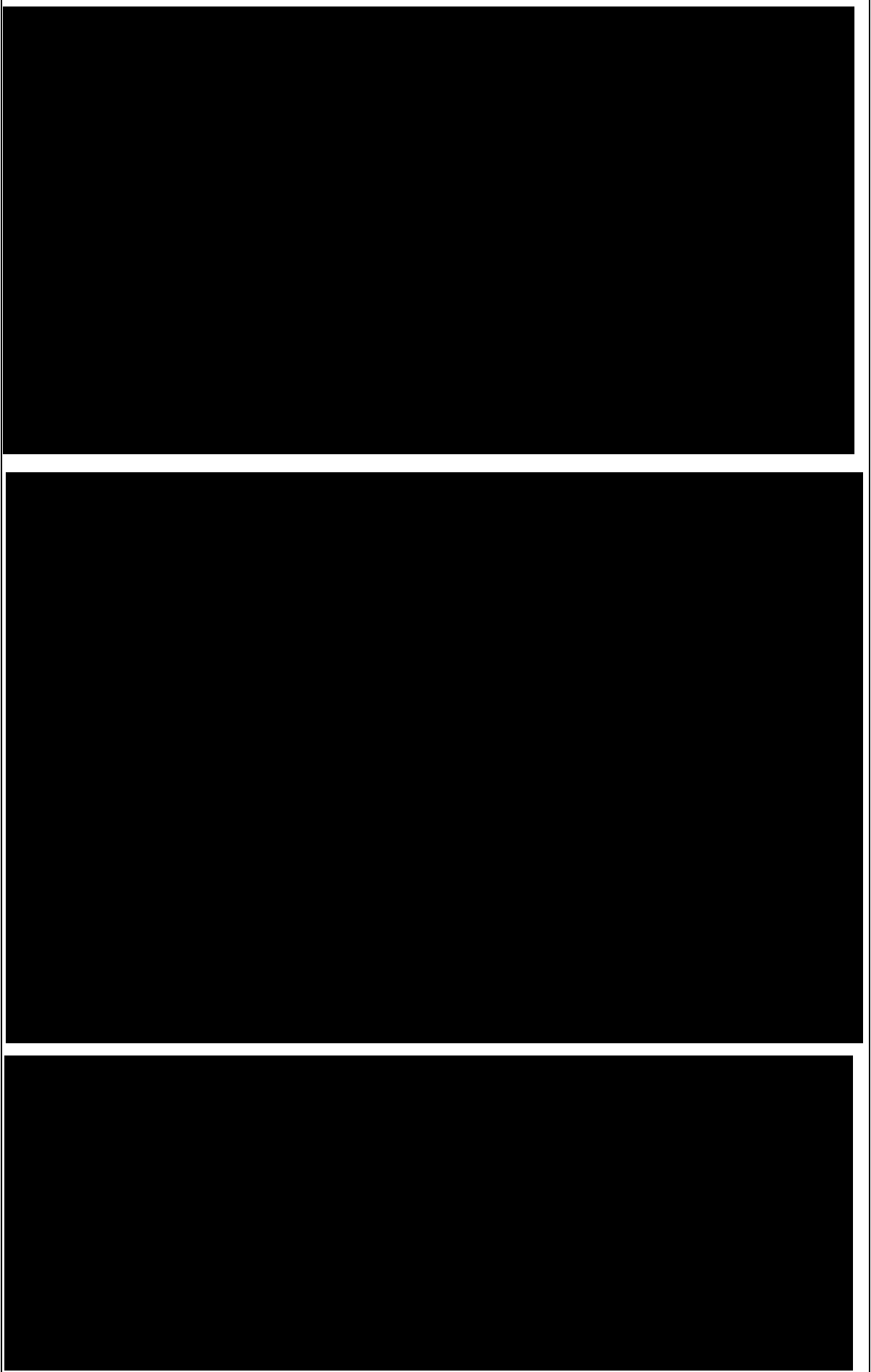
[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]

- [REDACTED]





[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] e

applicable.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]ent



SCHEDULE 3 – PRICE

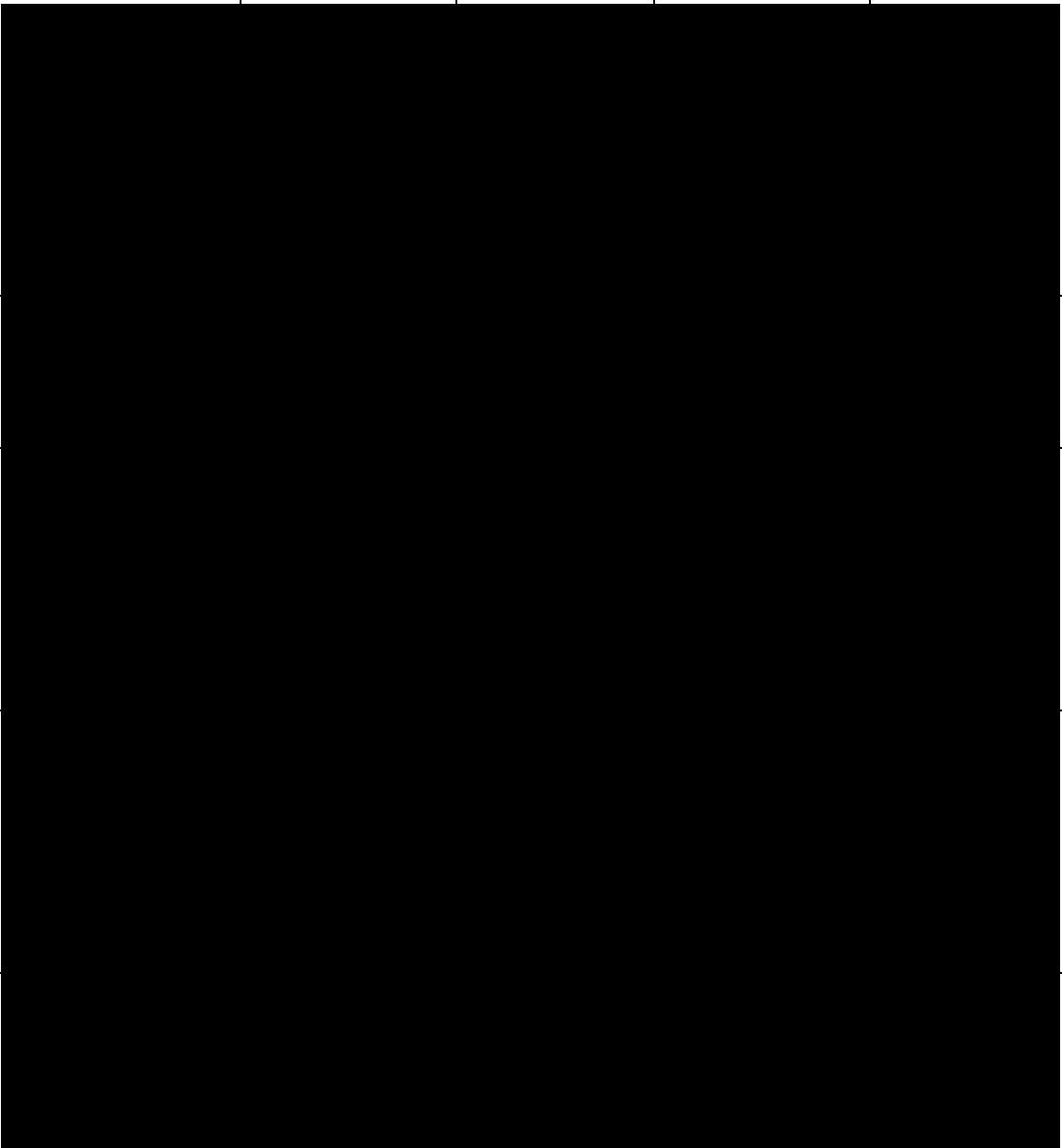
All invoices will be paid within 30 days of receipt. Invoices need to quote a valid PO number and sent to accountspayable@cqc.org.uk

Care Quality Commission
Citygate, Gallowgate
Newcastle upon Tyne
NE1 4PA

Below costs cover 2-year period

Item no	Module Name	Module Element	Unit Cost (excluding VAT)	Unit Cost (including VAT)	Total cost (excluding VAT)	Total cost (including VAT)
1.	Year 1: Initial kick-off & stakeholder meetings.					

2.	Year 1: Pre-training SMILE Survey and report.				
3.	Year 1: Focus Groups, line managers & remaining staff members.				
4.	Year 1: Content creation. (Including adjustments made based on feedback)				
5.	Year 1: Half-day Virtual training. (required 6 sessions)				
6.	Year 1: Half-day Face to face training. (required 6 sessions)				
7.	Year 1: Midway evaluation & in-depth report, with virtual feedback to key stakeholders.				

8.	Year 1 & 2: Regular stakeholder meetings & catch ups. (Amount to be confirmed during initial kick-off meeting)					
9.	Year 2: Half day Virtual training. (required 4 sessions)					
10.	Year 2: Half day Face to face training. (required 4 sessions)					
11.	Year 2: Half day Leadership development training Face to Face (required 4 sessions)					
	Year 2: Development and creation of E-learning Course (course duration of up to 1-hour of learning)					

12.	Year 2: E-learning development and implementation. (Licence with 90-days course content access for 190 staff)							
13.	Year 2: Post training SMILE survey and report.							
14.	Year 2: Final evaluation & in-depth report, with virtual feedback to key stakeholders.							
Total Cost							£139,400.00	£167,280.00

Please note the volumes are indicative only; CQC reserves the right to change at its discretion

ANNEX 1: TENDER CLARIFICATIONS

Clarification Question	Response
You mention wanting some eLearning in the specification - how have you come to this conclusion and what do you want it to achieve? Would you be open to alternatives as long as they come in under your budget?	This is to support different approaches to learning and have some core material that can be referred back to. Yes, we would be open to alternatives
In your pricing response document you are very clear about group sizes and the number of repeat sessions you are looking for - should this be used as a framework when completing the quality response covering delivery approach and methodology	Yes, this should be used as a framework to support the whole team to receive accessible training in group sizes to facilitate the learning and open discussion.
This is a 2-year funded programme, and you are very clear on your expected milestones for year 1 - what are your expectations for year 2?	These are dependent on Y1 delivery, there is a requirement to be flexible to support how this develops.
Would it be possible to clarify locations for face-to-face delivery will these be nationally. Would live online delivery via a platform such as zoom, or teams be accepted?	There is access to CQC offices which can be used in Stratford, London and Newcastle. The platform supported would be Teams.
For evaluation criteria 4 - Accessibility and Inclusion. We wondered are you aware of the existing accessibility requirements of your workforce so that we can write a more tailored response to this question?	We do have an understanding of the accessibility needs of the team, these relate to physical disability and reasonable adjustments. We would require there to be flexibility to support varied approaches to learning, an understanding we may request a bespoke request. Hybrid options to support digital and physical attendance.
Could we enquire as to why this tender is listed as 'not suitable for VCSEs'?	Apologies, the opportunity notice should have included VCSEs.
What are the percentages regards ethnic race in the team being trained? 2. Required Training: - Training up to 20 delegates – cost for 10 sessions,	Less than 10% There is some flexibility in this proposal.

<p>(both face to face and virtual). Are these 20 sessions for 20 delegates or is it 10 sessions for different team members up to 200 people? Or is it up to us, depending upon what we find is required. For example, does this mean we might deliver 10 x 4 hour sessions face to face, (the same session 10 times), and 10 x 2 hour sessions, (the same session 10 times) virtual dependent upon needs</p> <p>- Training – 30 colleagues with line management responsibilities - cost for 4 sessions. We prefer this is face to face due to the importance of Line Managers leading this? Is this a problem to bring them together?</p> <p>3. Focus Groups - cost for 4 sessions for line managers and 6-8 focus groups for remaining team. Is this online or face to face, or a combination of both. And, if we want to bring some of the groups together face to face, would that be possible?</p> <p>4. e-Learning - Is the expectation that this is a software programme, or rather short videos with workbooks?</p>	<p>No, we would prefer to bring line managers together</p> <p>Combination</p> <p>Yes</p> <p>Short videos / workbooks</p>
<p>1. If the whole team are remote workers, are you open to all of the training being remote? We are confident we can deliver high impact, interactive training online for the whole team in a much more cost-effective and time-efficient way for your staff than if they and us are required to travel to regional offices</p> <p>2. Of the 190 staff members how many of these are line managers and/or leaders?</p> <p>3, Are you looking for staff to take an anti racist approach in their working environment when engaging with staff and patients, or are you looking to go deeper than this and support them to take an anti racist approach to the investigations that they carry out?</p> <p>4. Are there any more details you can share on the MSNI programme's transformational change programme, and the initial diagnostic work around anti-racism that has taken place? If not, can we confirm that this will be shared with the chosen delivery partner?</p> <p>5. The ITT states that other approaches may be needed to support the specific needs of individuals. Are there any indications you can give on what some of these specific needs might be at this stage?</p> <p>6. Price response and approach - do you want us to outline how we would deliver (and give costs for) the</p>	<p>Our preference would be to do a combination of remote and in person.</p> <p>Approximately 30</p> <p>Both this work needs to inform the investigations we undertake as well as supporting the programme to embed an anti-racist approach in all areas.</p> <p>We are unable to share the preliminary diagnostic and would plan to share with the chosen provider.</p> <p>These may be 1:1 sessions or sessions with a defined group of individuals</p> <p>The number and types of sessions based on your experience.</p>

<p>exact number of sessions you have specified, or the number and types of sessions and numbers of attendees that we think will be most effective based on our experience?</p> <p>7. The evaluation criteria does not appear to include any evaluation of suppliers' relevant experience or examples of similar work delivered, should we include this as part of our submission or will this not be assessed?</p>	<p>Your relevant experience should be included</p>
<p>What's your ideal duration for i) virtual and ii) in-person sessions?</p>	<p>Virtual 2 hours, in person up to ½ day</p>
<p>Is it your intention that everyone will attend one in-person workshop and one virtual, or that each workshop is available as both in-person and virtual options?</p>	<p>They attend one of each</p>
<p>With regards to pricing, shall we treat the 4 Managers sessions as in-person or virtual?</p>	<p>In person</p>
<p>With regards to 30 managers and 4 sessions - is this all 30 managers attending 4 'modules' as one cohort or will this be smaller groups split across the four sessions?</p>	<p>Smaller groups split across 4 sessions</p>
<p>Are the manager sessions in addition to the 'all staff sessions' in order that everyone attends the first level training together and managers have additional training after? Or is it your intention that staff and managers attend different workshops?</p>	<p>We would like the managers to attend additional training before that informs their attendance at further sessions</p>
<p>As we have to include expenses in the quotation, it would be helpful to understand how many sessions in each location so all suppliers can quote like for like.</p>	<p>This needs to be an approximation as we would need to confirm location based on CQC office availability.</p>
<p>What relevant development has already been implemented.</p>	<p>Implementation of EDI lead role, updates and training within particular elements, preliminary diagnostics, work and access to wider CQC EDI training and networks.</p>
<p>Can we check that it's ok to exclude words within images in the word count?</p>	<p>Yes</p>
<p>Would you view relevant video content if included?</p>	<p>Yes</p>
<p>Would it be possible to extend the Appendices allowance to accept detailed programme content/outline (which we are unable to include within the 1500-word count) - we feel this would be beneficial in the comparison of submissions.</p>	<p>This should not exceed 2 pages</p>
<p>There is a significant overlap between the requirements of Q2 and Q3 with regards to monitoring and impact which is making it difficult to feel confident we are clear on your precise requirements for each question. Is it your intention for there to be overlap or might we need further clarification?</p>	<p>Yes there will be overlap within this work</p>

Similarly, Q4 is already covered in Q3 and to some extent Q2 as well. Can we again check it's your intention for that to be the case?	Yes there will be overlap and revisiting of information with variation to detail and granularity
Would it be possible to clarify what is meant by: 'Provide up to two examples of your reporting processes, including details of team progress and development'	Attendance and measurement of understanding
We haven't seen any of the usual 'tender' questions with regards to company details, 'persons of significant control', GDPR, case studies/references etc, etc - have we missed something, or can we confirm it is just Appendix C-G to return?	Only Appendix C-G are required at this stage. The contract will contain this information once awarded to the successful supplier.
In Appendix B Annex 1 we are asked to outline our security plan: is there a word limit or preferred format for this?	No, there is no word limit or preferred format.
In Appendix A, Is the proposed budget to cover the milestones up to month 12 in Feb / March 2026 or to also cover work up to March 2027?	The proposed budget of £160,000 to £180,000 Including VAT is to cover costs up to March 2027 (Initial 2 years)
Following the facilitation of focus groups and review of data collected, are you open to some pilot sessions of training to be run to further shape up learning objectives before a wider team rollout?	Yes
Regarding scheduling focus groups and training: will CQC MNSI work with the supplier to notify participants of their sessions, and support with additional internal comms to maximise engagement and impact in those sessions?	Yes, there will be alignment with the MNSI comms team
In addition to the work outlined in the ITT offered by the supplier, will CQC MNSI be offering further support to participants participating in the anti-racism initiative e.g. creating safe spaces for team mates to decompress after participating in focus groups and training?	We do have support mechanism in place such as debrief etc. We would equally be seeking support in this area
Are you able to share data on what percentage of team members with line management responsibilities are ethnic minorities?	Small numbers
What is the highest level of seniority expected to participate in this programme, and would you like to include a separate, tailored session for senior leaders to focus on their strategic role in embedding anti-racism?	All team members would be participating up to Director level. Yes, we would like to include senior leader tailored sessions.
Are there any existing staff networks, resource groups, or internal initiatives related to anti-racism, EDI, or psychological safety that we should consider aligning with or integrating into the programme?	There is an EDI lead within MNSI and connection with the EDI team in CQC alongside active networks across CQC.
We noticed that the tender questions do not ask about CVs or any qualifications of the project team. Is this something that can be included or attached?	Information about the project team's

	qualifications or CVs would be welcomed
Please can you clarify what you mean by Unit Cost in Appendix D e.g. do you want the hourly rate pricing for that type of work e.g. for a two-hour session, the price per hour. Or do you want a price per session e.g. total price for one focus group?	Can we have both as depending on the type of session we may want an hourly rate or a focus group rate
In both the Price Response Document and the clarifications, you've stated that employees would attend one 1/2-day in-person workshop and one 2-hour online workshop. Would you consider a more holistic approach requiring more F2F and online attendance over a longer period of time, as long as it stays within budget?	Yes
For evaluation question 1 "• Demonstrating how you will engage the wider team in deepening both individual and collective understanding of anti-racism." who are you referring to as the wider team please? can we have an understanding of the organisational structure, leaders, line managers, wider team, senior leaders and number in each tier/group	The wider team is those outside of line managers. This is approximately 170 team members
Is the expectation that all 190 receive training across the 2 years.	Yes
What percentage of people or number of people do you want participating in the focus groups please	This needs to be representative of the whole team and taking into consideration those who wish to participate. This needs to be 100% of each group asked and then the participation rate to be reviewed.
For evaluation question 4 do you want an answer of 100 words and in addition to that an accessibility statement of 2 A4 sides?	Yes
As you have said there are overlaps with the questions, will suppliers responses be read holistically or are we to repeat ourselves in different responses. I ask this given the word count for the questions.	Yes

SCHEDULE 4 – PROCESSING, PERSONAL DATA AND DATA SUBJECTS

- 1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller and the Contractor is the Processor. The only processing that the Processor is authorised to do is listed in Annex 1 to this Schedule 4 by the Controller and may not be determined by the Processor.
- 2 The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.
- 3 The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:
 - (a) a systematic description of the envisaged processing operations and the purpose of the processing;
 - (b) an assessment of the necessity and proportionality of the processing operations 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.
- 4 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Agreement:
 - (a) process that Personal Data only in accordance with Annex 1 to this Schedule 4, unless the Processor is required to do otherwise by Law. If it is so required 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 Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures), having taken account of the:
 - (i) nature of the data to be protected;
 - (ii) harm that might result from a Data Loss Event;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;
 - (c) ensure that :
 - (i) the Processor Personnel do not process Personal Data except in accordance with this Agreement (and in particular Annex 1 to this Schedule 4);

- (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
 - (A) are aware of and comply with the Processor's duties under this clause;
 - (B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;
 - (C) 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 Agreement; and
 - (D) have undergone adequate training in the use, care, protection and handling of Personal Data; and
- (d) not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
 - (i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;
 - (ii) the Data Subject has enforceable rights and effective legal remedies;
 - (iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); 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;
- (e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Agreement unless the Processor is required by Law to retain the Personal Data.

5 Subject to paragraph 6, the Processor shall notify the Controller immediately if it:

- (a) receives a Data Subject Access Request (or purported Data Subject Access Request);
- (b) receives a request to rectify, block or erase any Personal Data;
- (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
- (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;
- (e) 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

(f) becomes aware of a Data Loss Event.

- 6 The Processor's obligation to notify under paragraph 5 shall include the provision of further information to the Controller in phases, as details become available.
- 7 Taking into account the nature of the processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 5 (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 the Controller to comply with a Data Subject Request within the relevant timescales set out in the Data Protection Legislation;
 - (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;
 - (e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.
- 8 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this paragraph. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
 - (a) the Controller determines that the processing is not occasional;
 - (b) the Controller determines the processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or
 - (c) the Controller determines that the processing is likely to result in a risk to the rights and freedoms of Data Subjects.
- 9 The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
- 10 Each Party shall designate its own data protection officer if required by the Data Protection Legislation.
- 11 Before allowing any Sub-processor to process any Personal Data related to this Agreement, 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 give effect to the terms set out in this Schedule 14 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.

- 12 The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.
- 13 The Controller may, at any time on not less than 30 Working Days' notice, revise this paragraph by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).
- 14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on not less than 30 Working Days' notice to the Processor amend this agreement to ensure that it complies with any guidance issued by the Information Commissioner's Office.
- 15 Subject to clause 14.5, the Processor shall indemnify the Controller on a continuing basis against any and all Losses incurred by the Controller arising from the Processor's Default under this Schedule 4 and/or any failure by the Processor or any Sub-processor to comply with their respective obligations under Data Protection Legislation.
- 16 Nothing in this Schedule 4 shall be construed as requiring the Processor or any relevant Sub-processor to be in breach of any Data Protection Legislation.

ANNEX 1 – Data Processing Schedule

1. The contact details of the Controller's Data Protection Officer are: [REDACTED]
[REDACTED] Care Quality Commission, Citygate, Gallowgate, Newcastle
Upon Tyne, NE1 4PA, United Kingdom.

2. The contact details of the Processor's Data Protection Officer are: [REDACTED]
[REDACTED] Onyx House 12 Phoenix Business Park, Avenue Close,
Birmingham, England, B7 4NU

3. The Processor shall comply with any further written instructions with respect to processing by the Controller.

4. Any such further instructions shall be incorporated into this Schedule.

Description	Details
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Authority is the Controller, and the Contractor is the Processor in accordance with Clause E2.1
Subject matter of the processing	Anti -Racism Training
Duration of the processing	2 + 1 Years (if extended)
Nature and purposes of the processing	<ul style="list-style-type: none">• Records of attendance• Survey responses• Notes from training
Type of personal data	<ul style="list-style-type: none">• Name• Email address
Categories of Data Subject	<ul style="list-style-type: none">• Staff
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	Data relating to the training will be held to confirm attendance only. Survey responses etc will not be held post training.

SCHEDULE 5 – SECURITY REQUIREMENTS AND PLAN

INTERPRETATION AND DEFINITION

For the purposes of this Schedule 5, unless the context otherwise requires the following provisions shall have the meanings given to them below:

“Breach of Security” means the occurrence of unauthorised access to or use of the Premises, the Premises, the Services, the Contractor System, or any ICT or data (including Authority Data) used by the Authority or the Contractor in connection with the Contract.

“Contractor Equipment” means the hardware, computer and telecoms devices and equipment supplied by the Contractor or its Sub-Contractor (but not hired, leased or loaned from the Authority) for the provision of the Services;

“Contractor Software” means software which is proprietary to the Contractor, including software which is or will be used by the Contractor for the purposes of providing the Services and which is specified as such in Schedule 5.

“ICT” means Information Communications Technology and includes a diverse set of technological tools and resources used to communicate, and to create, disseminate, store and manage information, including computers, the Internet, broadcasting technologies (radio and television), and telephony.

“Protectively Marked” shall have the meaning as set out in HMG Security Policy Framework.

“Security Plan” means the Contractor’s security plan prepared pursuant to paragraph 3 an outline of which is set out in an Appendix to this Schedule 5.

“Software” means Specially Written Software, Contractor Software and Third Party Software.

“Specially Written Software” means any software created by the Contractor (or by a third party on behalf of the Contractor) specifically for the purposes of this Contract.

“Third Party Software” means software which is proprietary to any third party which is or will be used by the Contractor for the purposes of providing the Services including the software and which is specified as such in Schedule 7.

1. INTRODUCTION

This Schedule 5 covers:

- 1.1 principles of security for the Contractor System, derived from HMG Security Policy Framework, including without limitation principles of physical and information security;
- 1.2 wider aspects of security relating to the Services;
- 1.3 the creation of the Security Plan;
- 1.4 audit and testing of the Security Plan; and
- 1.5 breaches of security.

2. PRINCIPLES OF SECURITY

- 2.1 The Contractor acknowledges that the Authority places great emphasis on confidentiality, integrity and availability of information and consequently on the security of the Premises and the security for the Contractor System. The Contractor also acknowledges the confidentiality of Authority Data.

- 2.2 The Contractor shall be responsible for the security of the Contractor System and shall at all times provide a level of security which:
- 2.2.1 is in accordance with Good Industry Practice and Law;
 - 2.2.2 complies with HMG Security Policy Framework; and
 - 2.2.3 meets any specific security threats to the Contractor System.
- 2.3 Without limiting paragraph 2.2, the Contractor shall at all times ensure that the level of security employed in the provision of the Services is appropriate to maintain the following at acceptable risk levels (to be defined by the Authority):
- 2.3.1 loss of integrity of Authority Data;
 - 2.3.2 loss of confidentiality of Authority Data;
 - 2.3.3 unauthorised access to, use of, or interference with Authority Data by any person or organisation;
 - 2.3.4 unauthorised access to network elements, buildings, the Premises, and tools used by the Contractor in the provision of the Services;
 - 2.3.5 use of the Contractor System or Services by any third party in order to gain unauthorised access to any computer resource or Authority Data; and
 - 2.3.6 loss of availability of Authority Data due to any failure or compromise of the Services.
 - 2.3.7 processing and storage of authority data within the UK or by exception within the EEA. Any processing outside of the UK must be subject to specific approval by the Authority.

3. SECURITY PLAN

- 3.1 The Contractor shall develop, implement and maintain a Security Plan to apply during the Contract Period (and after the end of the term as applicable) which will be approved by the Authority, tested, periodically updated and audited in accordance with this Schedule 5.
- 3.2 A draft Security Plan provided by the Contractor as part of its bid is set out herein.
- 3.3 Prior to the Commencement Date the Contractor will deliver to the Authority for approval the final Security Plan which will be based on the draft Security Plan set out herein.
- 3.4 If the Security Plan is approved by the Authority it will be adopted immediately. If the Security Plan is not approved by the Authority the Contractor shall amend it within 10 Working Days of a notice of non-approval from the Authority and re-submit to the Authority for approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the Parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the Security Plan following its resubmission, the matter will be resolved in accordance with clause 19 (Dispute Resolution). No approval to be given by the Authority pursuant to this paragraph 3.4 may be unreasonably withheld or delayed. However any failure to approve the Security Plan on the grounds that it does not comply with the requirements set out in paragraphs 3.1 to 3.4 shall be deemed to be reasonable.

- 3.5 The Security Plan will set out the security measures to be implemented and maintained by the Contractor in relation to all aspects of the Services and all processes associated with the delivery of the Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with:
- 3.5.1 the provisions of this Schedule 5;
 - 3.5.2 the provisions of Schedule 1 relating to security;
 - 3.5.3 the Information Assurance Standards;
 - 3.5.4 the data protection compliance guidance produced by the Authority;
 - 3.5.5 the minimum set of security measures and standards required where the system will be handling Protectively Marked or sensitive information, as determined by the Security Policy Framework;
 - 3.5.6 any other extant national information security requirements and guidance, as provided by the Authority's IT security officers; and
 - 3.5.7 appropriate ICT standards for technical countermeasures which are included in the Contractor System.
- 3.6 The references to Quality Standards, guidance and policies set out in this Schedule shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such Quality Standards, guidance and policies, from time to time.
- 3.7 If there is any inconsistency in the provisions of the above standards, guidance and policies, the Contractor should notify the Authorised Representative of such inconsistency immediately upon becoming aware of the same, and the Authorised Representative shall, as soon as practicable, advise the Contractor which provision the Contractor shall be required to comply with.
- 3.8 The Security Plan will be structured in accordance with ISO/IEC27002 and ISO/IEC27001 or other equivalent policy or procedure, cross-referencing if necessary to other schedules of the Contract which cover specific areas included within that standard.
- 3.9 The Security Plan shall not reference any other documents which are not either in the possession of the Authority or otherwise specified in this Schedule 5.

4. AMENDMENT AND REVISION

- 4.1 The Security Plan will be fully reviewed and updated by the Contractor annually or from time to time to reflect:
- 4.1.1 emerging changes in Good Industry Practice;
 - 4.1.2 any change or proposed change to the Contractor System, the Services and/or associated processes;
 - 4.1.3 any new perceived or changed threats to the Contractor System;
 - 4.1.4 changes to security policies introduced Government-wide or by the Authority; and/or

4.1.5 a reasonable request by the Authority.

4.2 The Contractor will provide the Authority with the results of such reviews as soon as reasonably practicable after their completion and amend the Security Plan at no additional cost to the Authority.

4.3 Any change or amendment which the Contractor proposes to make to the Security Plan (as a result of an Authority request or change to Schedule 1 or otherwise) shall be subject to a Variation and shall not be implemented until Approved.

5. AUDIT, TESTING AND PROTECTIVE MONITORING

5.1 The Authority shall be entitled to send a representative to witness the conduct of the Security Tests. The Contractor shall provide the Authority with the results of such tests (in an Approved form) as soon as practicable after completion of each Security Test.

5.2 Without prejudice to any other right of audit or access granted to the Authority pursuant to the Contract, the Authority shall be entitled at any time and without giving notice to the Contractor to carry out such tests (including penetration tests) as it may deem necessary in relation to the Security Plan and the Contractor's compliance with and implementation of the Security Plan. The Authority may notify the Contractor of the results of such tests after completion of each such test. Security Tests shall be designed and implemented so as to minimise the impact on the delivery of the Services.

5.3 Where any Security Test carried out pursuant to paragraphs 5.1 or 5.2 reveals any actual or potential security failure or weaknesses, the Contractor shall promptly notify the Authority of any changes to the Security Plan (and the implementation thereof) which the Contractor proposes to make in order to correct such failure or weakness. Subject to Approval in accordance with paragraph 4.3, the Contractor shall implement such changes to the Security Plan in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the Security Plan to address a non-compliance with HMG Security Policy Framework or security requirements, the change to the Security Plan shall be at no additional cost to the Authority. For the purposes of this paragraph, a weakness means a vulnerability in security and a potential security failure means a possible breach of the Security Plan or security requirements.

6. BREACH OF SECURITY

6.1 Either Party shall notify the other immediately upon becoming aware of any Breach of Security including, but not limited to an actual, potential or attempted breach, or threat to, the Security Plan.

6.2 Upon becoming aware of any of the circumstances referred to in paragraph 6.1, the Contractor shall immediately take all reasonable steps necessary to:

6.2.1 remedy such breach or protect the Contractor System against any such potential or attempted breach or threat; and

6.2.2 prevent an equivalent breach in the future;

6.2.3 collect, preserve and protect all available audit data relating to the incident and make it available on request to the Authority;

6.2.4 investigate the incident and produce a detailed report for the Authority within 5 working days of the discovery of the incident.

- 6.3 Such steps shall include any action or changes reasonably required by the Authority. If such action is taken in response to a breach that is determined by the Authority acting reasonably not to be covered by the obligations of the Contractor under the Contract, then the Contractor shall be entitled to refer the matter to the variation procedure set out in the Contract.
- 6.4 The Contractor shall as soon as reasonably practicable provide to the Authority full details (using such reporting mechanism as may be specified by the Authority from time to time) of such actual, potential or attempted breach and of the steps taken in respect thereof.

7. CONTRACT EXIT – SECURITY REQUIREMENTS

In accordance with clause 16 of the Contract, on termination of the Contract, either via early termination or completion of the Contract then the Contractor will either return all data to the Authority or provide a certificate of secure destruction using an industry and Authority approved method. Destruction or return of the data will be specified by the Authority at the time of termination of the Contract.

APPENDIX 1- OUTLINE SECURITY PLAN

ANNEX 1: BASELINE SECURITY REQUIREMENTS

1. SECURITY CLASSIFICATION OF INFORMATION

- 1.1 If the provision of the Services requires the Contractor to Process Authority Data which is classified as OFFICIAL, OFFICIAL-SENSITIVE or Personal Data, the Contractor shall implement 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 legislative and regulatory obligations.

2. END USER DEVICES

- 2.1 The Contractor shall ensure that any Authority which resides on a mobile, removable or physically uncontrolled device is stored encrypted using a product or system component which has been formally assured through a recognised certification process agreed with the Authority except where the Authority has given its prior written consent to an alternative arrangement.
- 2.2 The Contractor shall ensure that any device which is used to Process Authority Data meets all of the security requirements set out in the NCSC End User Devices Platform Security Guidance, a copy of which can be found at: <https://www.ncsc.gov.uk/guidance/end-user-device-security>.

2A. TESTING

The Contractor shall at their own cost and expense, procure a CHECK or CREST Certified Contractor to perform an ITHC or Penetration Test prior to any live Authority data being transferred into their systems. The ITHC scope must be agreed with the Authority to ensure it covers all the relevant parts of the system that processes, stores or hosts Authority data.

3. DATA PROCESSING, STORAGE, MANAGEMENT AND DESTRUCTION

- 3.1 The Contractor and Authority recognise the need for the Authority's information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Contractor must be able to state to the Authority the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Authority Data will be subject to at all times.
- 3.2 The Contractor shall not, and shall procure that none of its Sub-contractors, process Authority Data outside the EEA without the prior written consent of the Authority and the Contractor shall not change where it or any of its Sub-contractors process Authority Data without the Authority's prior written consent which may be subject to conditions.
- 3.3 The Contractor must be able to demonstrate they can supply a copy of all data on request or at termination of the service, and must be able to securely erase or destroy all data and media that the Authority data has been stored and processed on.

The Contractor shall:

- 3.3.1 provide the Authority with all Authority Data on demand in an agreed open format;
- 3.3.2 have documented processes to guarantee availability of Authority Data in the event of the Contractor ceasing to trade;
- 3.3.3 securely destroy all media that has held Authority Data at the end of life of that media in line with Good Industry Practice; and
- 3.3.4 securely erase any or all Authority Data held by the Contractor when requested to do so by the Authority.

4. NETWORKING

- 4.1 The Authority requires that any Authority Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted when transmitted.

- 4.2 The Authority requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5. SECURITY ARCHITECTURES

- 5.1 Contractors should design the service in accordance with:
- NCSC " Security Design Principles for Digital Services "
 - NCSC " Bulk Data Principles "
 - NSCS " Cloud Security Principles "

6. PERSONNEL SECURITY

- 6.1 All Contractor Personnel shall be subject to a pre-employment check before they may participate in the provision and or management of the Services. Such pre-employment checks must include all pre-employment checks which are required by the HMG Baseline Personnel Security Standard or equivalent including: verification of the individual's identity; verification of the individual's nationality and immigration status; and, verification of the individual's employment history; verification of the individual's criminal record. The Contractor maybe required implementing additional security vetting for some roles.

7. IDENTITY, AUTHENTICATION AND ACCESS CONTROL

- 7.1 The Contractor must operate an appropriate access control regime to ensure that users and administrators of the service are uniquely identified. The Contractor must retain records of access to the physical sites and to the service.

8. AUDIT AND PROTECTIVE MONITORING

- 8.1 The Contractor shall collect audit records which relate to security events in delivery of the service or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Contractor audit records should (as a minimum) include:

- 8.1.1 regular reports and alerts setting out details of access by users of the service, 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. The retention periods for audit records and event logs must be agreed with the Authority and documented.

- 8.2 The Contractor and the Authority shall work together to establish any additional audit and monitoring requirements for the ICT Environment.
- 8.3 The Contractor shall retain audit records collected in compliance with this Paragraph 8.3 for a period of at least 6 months.

9. VULNERABILITIES AND CORRECTIVE ACTION

- 9.1 Contractors shall procure and implement security patches to vulnerabilities in accordance with the timescales specified in the NCSC Cloud Security Principle 5.

- 9.2 Contractor must ensure that all COTS Software and Third Party COTS Software be kept up to date such that all Contractor COTS Software and Third Party COTS Software are always in mainstream support.
- 10. RISK ASSESSMENT**
- 10.1 The Contractor should perform a technical information risk assessment on the service supplied and be able to demonstrate what controls are in place to address those risks.

ANNEX 2: CONTRACTOR'S SECURITY MANAGEMENT PLAN

. Introduction

Mission Diverse is committed to the secure, lawful, and responsible management of information throughout the delivery of its training and consultancy services internally and to third-party organisations. This Security Management Plan outlines the comprehensive

framework that Mission Diverse adopts to ensure the confidentiality, integrity, and availability of information entrusted to it.

This Plan is designed to align with Good Industry Practice, the HMG Security Policy Framework, the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

The Plan sets out the governance arrangements, roles and responsibilities, detailed security controls, and operational practices Mission Diverse employs to manage and mitigate information security risks. All Mission Diverse employees, associates, contractors, and third-party service providers are required to comply with the provisions outlined in this Security Management Plan as a condition of their engagement.

2. Definitions

For the purposes of this Security Management Plan:

- A “*Breach of Security*” refers to the unauthorised access to, use of, or interference with the Premises, the Contractor System, Services, or Authority Data.
- “*Contractor System*” means any system, equipment, or infrastructure used by Mission Diverse to deliver its services.
- “*Authority Data*” refers to all data provided by the client or generated during the provision of services, which must be safeguarded as confidential.
- “*Protectively Marked Information*” refers to data classified as OFFICIAL, OFFICIAL-SENSITIVE, or higher under the HMG Security Policy Framework.

Other definitions as necessary are derived directly from the standards referenced within this document.

3. Purpose of the Security Management Plan

The purpose of the Security Management Plan is to ensure that Mission Diverse manages all aspects of information security in a consistent, controlled, and legally compliant manner.

The Plan provides assurance to clients that their data will be protected against unauthorised access, loss, or disclosure during all phases of service delivery, and that appropriate measures are in place to detect, respond to, and recover from security incidents.

This Plan also supports Mission Diverse’s commitment to continuous improvement in information security practices and helps maintain trust with clients, partners, employees, and regulators.

4. Scope of the Plan

This Security Management Plan applies to all services provided by Mission Diverse, including in-person and online training sessions, consultancy engagements, research projects, and advisory services. It covers all information assets, ICT systems, employees, contractors, associates, and third-party providers involved in service delivery.

The Plan also applies to all physical locations used for service delivery, including Mission Diverse offices, client premises, temporary training venues, and remote work environments.

5. Security Governance Structure

Mission Diverse has established a robust security governance framework. The Data Protection Officer, currently Cleopatra Morris, ensures that all processing of Authority Data complies with data protection legislation and acts as the main liaison point for clients and regulatory authorities.

The Managing Director, Cleopatra Morris, oversees strategic security planning and allocates appropriate resources to support security initiatives. All Mission Diverse personnel, including associates and contractors, are individually responsible for complying with this Plan and reporting any security incidents or concerns promptly.

6. Information Classification and Handling

Mission Diverse classifies all information it handles into four categories: Public, Internal, Confidential, and Highly Confidential.

Where Authority Data is designated as OFFICIAL or OFFICIAL-SENSITIVE under HMG guidelines, additional controls are applied, including restricted access, encryption, and secure storage.

Mission Diverse ensures that sensitive information is only accessible to authorised individuals and that all transmission of such data is carried out using secure methods such as encrypted email or secure file transfer platforms. Printed copies of sensitive information are stored securely and destroyed using certified confidential waste disposal services when no longer required.

7. Physical and Premises Security

All Mission Diverse offices and facilities used in service delivery are secured against unauthorised access. Access to premises is controlled through locks, alarms, and visitor management protocols.

Sensitive information and IT equipment are stored securely when not in use. When delivering services at client sites or temporary venues, Mission Diverse complies fully with all local security procedures and conducts risk assessments to verify the adequacy of physical security measures.

8. Personnel Security

Mission Diverse ensures that all employees, contractors, and associates undergo pre-employment checks in line with Baseline Personnel Security Standard. These checks include verification of identity, nationality and immigration status, employment history, and criminal record where appropriate.

All personnel are required to sign confidentiality agreements prior to accessing Authority Data. Mandatory security awareness training is provided on induction and refreshed annually to ensure continued understanding of security responsibilities. Additional security vetting may be conducted where the nature of the service requires it.

9. Systems and ICT Security

Mission Diverse enforces strong technical security controls across all IT systems. All devices used for processing Authority Data are encrypted and protected using security solutions formally assured through recognised UK certification processes. Access to systems is tightly controlled through strong passwords, two-factor authentication, and strict access rights management.

User privileges are reviewed regularly to ensure access remains appropriate to role-based requirements. All software is kept up to date through regular patching, and all systems undergo vulnerability scans and penetration testing by CREST or CHECK-certified providers prior to handling live Authority Data. Data is transmitted securely across public and private networks using encryption technologies compliant with NCSC guidelines.

10. Data Processing, Storage, Management, and Destruction

Mission Diverse processes and stores Authority Data exclusively within secure environments located in the United Kingdom or, with prior written consent, within the European Economic Area (EEA).

No Authority Data will be processed or stored outside these locations without explicit client approval. Mission Diverse maintains detailed documentation of data storage locations and the applicable legal frameworks governing such storage.

At the conclusion of a contract, Authority Data is either returned to the client in an agreed format or securely destroyed using certified methods. Certificates of destruction are issued where appropriate. Data destruction procedures ensure that media containing Authority Data is rendered unreadable and unrecoverable at the end of its lifecycle.

11. Risk Management and Technical Risk Assessments

Mission Diverse performs regular technical risk assessments to identify threats to the confidentiality, integrity, and availability of Authority Data. Each risk assessment identifies controls that are proportionate to the identified risks and aligned to industry standards.

Risk assessments are reviewed annually or whenever there are significant changes to the Contractor System, services, or security landscape. Findings and corrective actions are documented and tracked through to resolution.

12. Vulnerability Management and Corrective Action

Mission Diverse maintains a proactive vulnerability management programme. Security patches are applied to critical vulnerabilities in line with the timelines specified in the NCSC Cloud Security Principle 5.

All Commercial Off-the-Shelf (COTS) Software and Third-Party COTS Software used by Mission Diverse remains within mainstream vendor support, ensuring that software is actively maintained and secured against emerging threats.

13. Identity, Authentication, and Access Control

Mission Diverse ensures that all users of its systems are uniquely identified and authenticated. Robust access control policies ensure that users are granted the minimum level of access required for their role. Access records are maintained for both physical sites and digital systems to enable forensic investigation if necessary.

14. Audit, Monitoring, and Protective Monitoring

Mission Diverse collects and retains audit records related to security events, user activity, and administrative actions within its systems. Audit logs are maintained for a minimum period of six months and retained securely.

Regular analysis of audit records is performed to identify unusual patterns of access, potential breaches, or other security anomalies. Findings are reported internally to the Security Lead and corrective action is taken where required.

Mission Diverse cooperates fully with any client requirements for additional audit or monitoring activities related to the ICT environment supporting service delivery.

15. Audit, Testing, and Authority Oversight

Mission Diverse acknowledges the right of the client to conduct audits, inspections, and penetration testing activities at any time during the contract period. Where a security weakness or failure is identified, Mission Diverse will take immediate corrective action and, where necessary, update the Security Management Plan accordingly. All changes made in response to identified vulnerabilities are subject to client approval and verification.

16. Breach of Security and Incident Management

If Mission Diverse becomes aware of a Breach of Security, it will immediately notify the client's designated representative. Mission Diverse will take all reasonable steps to contain, mitigate, and investigate the breach without delay.

All audit data relating to the incident will be preserved and provided to the client on request. A detailed incident report, outlining the cause, impact, and remedial actions taken, will be

delivered within five working days of incident discovery. Mission Diverse will implement further measures to prevent recurrence and cooperate fully with any external investigations if required.

17. Contract Exit and Data Handover

At the termination of the contract, Mission Diverse will securely return all Authority Data to the client or will securely destroy the data using methods approved by the client.

Data destruction processes will be evidenced through the provision of formal Certificates of Secure Destruction. Mission Diverse ensures that no copies of Authority Data remain on any system, backup media, or archive unless otherwise agreed in writing with the client.

Mission Diverse is committed to maintaining the highest standards of information security across all aspects of its service delivery.

Through the implementation of this Security Management Plan, Mission Diverse demonstrates its proactive approach to risk management, legal compliance, client assurance, and operational resilience. This Plan will be reviewed annually, and updated whenever necessary, to ensure it remains aligned with evolving risks, legal requirements, and client expectations. All personnel and partners working on behalf of Mission Diverse are required to adhere fully to the provisions outlined within this Plan.

SCHEDULE 6 – CHANGE CONTROL

Contract Change Note

Contract Change Note Number	
Contract Reference Number & Title	
Variation Title	
Number of Pages	

WHEREAS the Contractor and the Authority entered into a Contract for the supply of [project name] dated [dd/mm/yyyy] (the "Original Contract") and now wish to amend the Original Contract

IT IS AGREED as follows

1. The Original Contract shall be amended as set out in this Change Control Notice:

Change Requestor / Originator		
Summary of Change		
Reason for Change		
Revised Contract Price	Original Contract Value	£
	Previous Contract Changes	£
	DN: Enter all CCN's here so that total value is shown for Audit purposes	
	Contract Change Note [x]	£
	New Contract Value	£
Revised Payment Schedule		
Revised Specification (See Annex [x] for Details)		
DN: Any change to Specification should be added as an Annex to the CCN		
Revised Term/Contract Period		
Change in Contract Manager(s)		
Other Changes		

2. Save as herein amended all other terms of the Original Contract shall remain effective.
3. This Change Control Notice shall take effect on [INSERT DATE] or from the date on which both the Authority and the Contractor have communicated acceptance of its terms.

SIGNED ON BEHALF OF THE AUTHORITY:	SIGNED ON BEHALF OF THE CONTRACTOR:
Signature:	Signature:

Name:	Name:
Position:	Position:
Date:	Date:

SCHEDULE 7 – THIRD PARTY SOFTWARE

CONTRACTOR SOFTWARE

For the purposes of this Schedule 7, “**Contractor Software**” means software which is proprietary to the Contractor, including software which is or will be used by the Contractor for the purposes of providing the Services. The Contractor Software comprises the following items:

Software	Contractor (if Affiliate of the Contractor)	Purpose	No. of Licences	Restrictions	No. of copies	Other	To be deposited in escrow?

THIRD PARTY SOFTWARE

For the purposes of this Schedule 7, “**Third Party Software**” means software which is proprietary to any third party which is or will be used by the Contractor for the purposes of providing the Services including the software specified in this Schedule 7. The Third Party Software shall consist of the following items:

Third Party Software	Contractor	Purpose	No. of Licences	Restrictions	No. of copies	Other	To be deposited in escrow?

SCHEDULE 8 – EXIT MANAGEMENT STRATEGY

To be mutually agreed by both parties