



www.cqc.org.uk

Contract (Short Form – Services)

Contract for the provision of Management/Leadership and Personal Development Online Learning Resources

Contract Reference CQC LD 177

June 2019

Contents

1	Interpretation.....	2
2	Priority of documents	6
3	Supply of Services	7
4	Term	7
5	Charges, Payment and Recovery of Sums Due	8
6	Premises and equipment	9
7	Staff and Key Personnel	10
8	Assignment and sub-contracting.....	11
9	Intellectual Property Rights	12
10	Governance and Records.....	13
11	Confidentiality, Transparency and Publicity	13
12	Freedom of Information	15
13	Protection of Personal Data.....	15
13A	Security	19
14	Liability and Insurance.....	19
15	Force Majeure	20
16	Termination	21
17	Compliance	22
18	Prevention of Fraud, Corruption and Bribery	23
19	Dispute Resolution	23
20	General.....	24
21	Notices	26
22	Governing Law and Jurisdiction	26
23	TUPE.....	27
	SCHEDULE 1 – INVITATION TO TENDER AND SPECIFICATION	28

SCHEDULE 2 – CHARGES30

SCHEDULE 3 – TENDER RESPONSE.....32

SCHEDULE 4 – PROCESSING, PERSONAL DATA AND DATA SUBJECTS49

SCHEDULE 5 – SECURITY REQUIREMENTS AND PLAN52

SCHEDULE 6 – CHANGE CONTROL73

SCHEDULE 7 – THIRD PARTY SOFTWARE74

SCHEDULE 8 – EXIT MANAGEMENT STRATEGY75

THIS CONTRACT is dated 26th of June 2019

PARTIES

- (1) **CARE QUALITY COMMISSION** of 151 Buckingham Palace Road, London, SW1W 9SZ ("**Authority**")

and

- (2) **MIND TOOLS LTD** of Pondtail Farm, West Grinstead, Horsham, RH13 8LN – 04829074 ("**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. CQC has adopted the 70/20/10 model of learning delivery and as such drives to ensure that our learning management system managed by the CQC Academy has appropriate content to build self-awareness and support self-guided learning.

In order to achieve this we need to ensure that we have sufficient learning resources available to support just in time self-directed learning and is reflective of how adult learners undertake development.

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 Specifications.

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:

- (a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are: (i) supplied to the Contractor by or on behalf of the Authority; or (ii) which the Contractor is required to generate, process, store or 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 any incident that result in unauthorised access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms;

"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:

- (a) Government Department;
- (b) Non-Departmental Public Body or Assembly Sponsored Public

Body (advisory, executive, or tribunal);

(c) Non-Ministerial Department; or

(d) Executive Agency;

"Charges" means the charges for the Services as specified in the Schedule 2;

"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;

"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;

"Data Controller, Data 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 of Personal Data in 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;
"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 Information Commissioner or relevant government department in relation to such legislation;
"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>);
"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 code of practice, judgment of a relevant court of law, or directives or requirements of any Regulatory Body with which the Contractor is bound to comply;
"Loss"	means any losses, costs, charges, expenses, interest, fees (including legal fees), payments, demands, liabilities, claims, proceedings, actions, penalties, charges, fines, damages, destruction, adverse judgments, orders or other sanctions and the term "Losses" shall be construed accordingly;
"LED"	means Law Enforcement Directive (<i>Directive (EU) 2016/680</i>)
"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;
"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, officers, employees, agents, consultants and contractors of the Processor and/or of any Sub-Processor engaged in the performance of its obligations under this Contract;
"Protective Measures"	means appropriate technical and organisational measures which include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the 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;
"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;
"Services"	means the services to be supplied by the Contractor to the Authority under the Contract;
"Specification"	means the specification for the Services (including as to quantity, description and quality) as specified in the 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 of the Contractor's 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-processor"	means any third Party appointed to process Personal Data on behalf of the Processor related to this Contract;
"Contractor Code"	means the HM Government Contractor Code of Conduct dated September

of Conduct" 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;

"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 Charges 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 Charges, 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 Charges 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 the 26th June 2019 and shall expire on the 20th August 2020, 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 10 Working Days' 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.
- 4.3 Content Customisation Start date - 26th June 2019

Subscription Period - 12 months

Subscription Start Date - 21st August 2019

If required, renewal date - 21st August 2020

Max Number of users - 3300

5 Charges, Payment and Recovery of Sums Due

- 5.1 The Charges for the Services shall be as set out in the Award Letter appended hereto 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 Charges 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 the Contract. 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 Contractor 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 materials created or developed by the Contractor pursuant to the Contract or arising as a result of the provision of the Services shall vest in the Authority. If, and to the extent, that any intellectual property rights in such materials vest in the Contractor by operation of law, the Contractor hereby assigns to the Authority by way of a present assignment of future rights that shall take place immediately on the coming into existence of any such intellectual property rights all its intellectual property rights in such materials (with full title guarantee and free from all third party rights).

9.3 The Contractor hereby grants the Authority:

9.3.1 a perpetual, royalty-free, irrevocable, non-exclusive licence (with a right to sub-license) to use all intellectual property rights in the materials created or developed pursuant to the Contract and any intellectual property rights arising as a result of the provision of the Services; and

9.3.2 a perpetual, royalty-free, irrevocable and non-exclusive licence (with a right to sub-license) to use:

a) any intellectual property rights vested in or licensed to the Contractor on the date of the Contract; and

b) any intellectual property rights created during the Term but which are neither created or developed pursuant to the Contract nor arise as a result of the provision of the Services,

including any modifications to or derivative versions of any such intellectual property rights, which the Authority reasonably requires in order to exercise its rights and take the benefit of the Contract including the Services provided.

- 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 Personal Data

- 13.1 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 Schedule 4 by the Controller and may not be determined by the Processor.
- 13.2 The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

- 13.3 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.
- 13.4 The Processor shall, in relation to any Personal Data processed in connection with its obligations under this Contract:
- (a) process that Personal Data only in accordance with Schedule 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 Contract (and in particular 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 Contract; 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 Contract unless the Processor is required by Law to retain the Personal Data.

- 13.5 Subject to clause 13.6, the Processor shall notify the Controller immediately if it:
- (a) receives a Data Subject Request (or purported Data Subject 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 Contract;
 - (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.
- 13.6 The Processor's obligation to notify under clause 13.5 shall include the provision of further information to the Controller in phases, as details become available.
- 13.7 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 clause 13.5 (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.

- 13.8 The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this clause. 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.
- 13.9 The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
- 13.10 Each Party shall designate its own data protection officer if required by the Data Protection Legislation.
- 13.11 Before allowing any Sub-processor to process any Personal Data related to this Contract, the Processor must:
- (a) notify the Controller in writing of the intended Sub-processor and processing;
 - (b) obtain the written consent of the Controller;
 - (c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this clause 13 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.
- 13.12 The Processor shall remain fully liable for all acts or omissions of any of its Sub-processors.
- 13.13 The Controller may, at any time on not less than 30 Working Days' notice, revise this clause 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 Contract).
- 13.14 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.
- 13.15 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 clause 13 and/or any failure by the Processor or any Sub-processor to comply with their respective obligations under Data Protection Legislation.
- 13.16 Nothing in this clause 13 shall be construed as requiring the Processor or any relevant Sub-processor to be in breach of any Data Protection Legislation.
- 13.17 The provision of this clause 13 applies during the Term and indefinitely after its expiry.

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 Charges 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 Charges paid or payable to the Contractor
 - 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 18.3 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 £80,000.

14.6 The Contractor shall hold:

- a) Employer's liability insurance 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 five million pounds (£5,000,000);
- c) Professional indemnity with the minimum cover per claim of five million pounds (£5,000,000);

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 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 and 17; 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 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, 16.6, 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.

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

16.6.1 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

16.6.2 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:

Address: 151 Buckingham Palace Road, London, SW1W 9SZ

For the attention of: [REDACTED]

Tel: [REDACTED]

Email: [REDACTED]

21.3.2 For the Contractor:

Address: Mind Tools Ltd, The Hay Barn, Pondtail Farm, Horsham, RH123 8LN

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 on the date first above written.

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

Signature

Name

Position

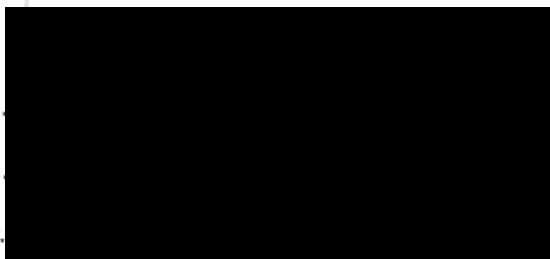


SIGNED for and on behalf of **MIND TOOLS LTD**

Signature

Name

Position



SCHEDULE 1 – INVITATION TO TENDER AND SPECIFICATION

Background

The Care Quality Commission (CQC) is the regulator of health and social care in England, inspecting health and social care services across the country. The Commission is split into five directorates: Adult Social Care, Hospitals and Mental Health, Primary Medical Services, Strategy and Intelligence and Customer and Corporate Services.

CQC has adopted the 70/20/10 model of learning delivery and as such drives to ensure that our learning management system managed by the CQC Academy has appropriate content to build self-awareness and support self-guided learning.

In order to achieve this we need to ensure that we have sufficient learning resources available to support just in time self-directed learning and is reflective of how adult learners undertake development.

We recognise that a significant population for this learning is our leaders and managers however we also require learning resources that all our workforce can access and undertake to support their personal development.

Our management population is approximately 700 and a full workforce of 3300.

Specification

We seek to procure quality learning resources that enable just in time development in such areas as:

- **Leadership Skills including:**
 - General Leadership Models and Style (learning content and self - assessment tools)
 - Strategic Leadership
 - Emotional Intelligence
 - Power
 - Change Management (including the people management element of this)
- **Individual and Team Management including:**
 - Performance Management
 - Project Management (from a leadership perspective)
 - Digital Awareness
 - People and Team development
 - Risk Analysis and Management

- **Learning and Personal Development (e.g. Learning to Learn/ Personal Development) including**
 - Tools to build self-awareness
 - Presentation Skills
 - Time Management
 - Digital Awareness
 - Problem Solving
 - Stress and Resilience
 - Learning to Learn

These learning resources would need to be compatible with our Learning Management System (LMS). Specifically, this means that they must be SCORM 1.2, SCORM 2004 (1st, 2nd or 3rd edition) or AICC v3.5 compliant.

Although these do not necessarily need to sit within our LMS they do need to be capable of being accessed through this and provide tracking/ completion data.

SCHEDULE 2 – CHARGES

Item no	Module Name	Module Element	Unit Cost (including VAT)	Number required	Total cost (including VAT)
1.	Leadership Skills	General Leadership Models and Style (learning content and self - assessment tools)			
2.	Leadership Skills	Strategic Leadership			
3.	Leadership Skills	Emotional Intelligence			
4.	Leadership Skills	Power			
5.	Leadership Skills	Change Management (including the people management element of this)			
6.	Individual and Team Management	Performance Management			
7.	Individual and Team Management	Project Management (from a leadership perspective)			
8.	Individual and Team Management	Digital Awareness			
9.	Individual and Team Management	People and Team development			
10.	Individual and Team Management	Risk Analysis and Management			

11.	Learning and Personal Development (e.g. Learning to Learn/ Personal Development) including	Tools to build self-awareness	
12.	Learning and Personal Development (e.g. Learning to Learn/ Personal Development) including	Presentation Skills	
13.	Learning and Personal Development (e.g. Learning to Learn/ Personal Development) including	Time Management	
14.	Learning and Personal Development (e.g. Learning to Learn/ Personal Development) including	Digital Awareness	
15.	Learning and Personal Development (e.g. Learning to Learn/ Personal Development) including	Problem Solving	
16.	Learning and Personal Development (e.g. Learning to Learn/ Personal Development) including	Stress and Resilience	
17	Learning and Personal Development (e.g. Learning to Learn/ Personal Development) including	Learning to Learn	

SCHEDULE 3 – TENDER RESPONSE

Technical Standards

Mind Tools can integrate with any Single Sign-On system that you currently use, allowing your learners to access all our content through your existing login portal. Learners don't need to create a new profile or remember new details, through the unique identifier provided by you they would be able to gain access to the resources along with their Personal Learning Plan.

To set this up we would need the name of your Identity Provider, (IDP) and a little additional technical information, then our technical department will do the rest.

Once into your systems, the employee would access the Mind Tools resources and tools through 'deep links' located on your Cornerstone LMS, HRMS or Intranet system (or all three).

The 'deep links' work as entry points to the Mind Tools product enabling you to sign-post your learners to specific resources, or areas of the Mind Tools library from anywhere within your chosen platform; creating a learning journey that can be tailored to the need of your audience and tracked by our reporting hub.

Our resource directory provides a payload with deep links within them that authenticates the user and takes them to a specific resource. Mind Tools is not about completion rates, more providing a support mechanism to the user at a point of need and on demand – hence why we also provide a reporting dashboard so that you can see what your users are naturally gravitating towards, and this can be downloaded in a .CSV file and imported into your dashboards.

At present our resources are not SCORM compliant but this is a current project for our developers. However, having said that you will be able to set the Cornerstone LMS so that it marks the deep links as 'completed' at point of entry for the users.

As well as the Mind Tools App (downloaded from Apple App Store or Google Play) we also fully support:

- Chrome (Windows, Mac) Up-to-date Versions
- Firefox (Windows, Mac) Up-to-date Versions
- Safari (Mac) Up-to-date Versions
- Microsoft Edge (Windows) Up-to-date Versions
- IE11 (Windows

Track learner progress

The CQC would have access to the Mind Tools Reporting Client Dashboard where data can be viewed at a glance, with the ability to dive deeper into each area to break down the information further.

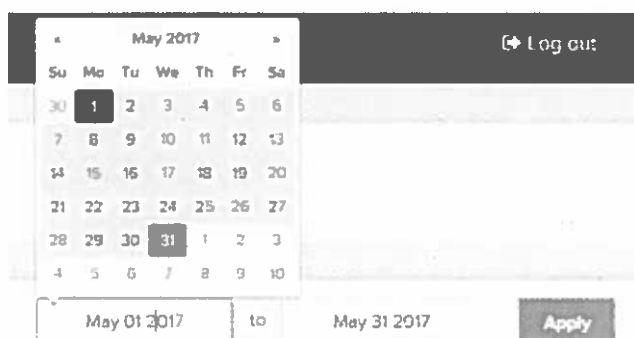
You can use Dashboard to discover key pieces of information such as number of active users, page views, what skill areas your learners are looking at and which resources are most popular. It also collects data from those users accessing Mind Tools from a mobile or tablet device.

This is updated daily and all of which can be downloaded as a .CSV file.

Your Client Success Manager will also always be there to tie this data to specific metrics to support a strategic business case and assist with any Administrative issues.



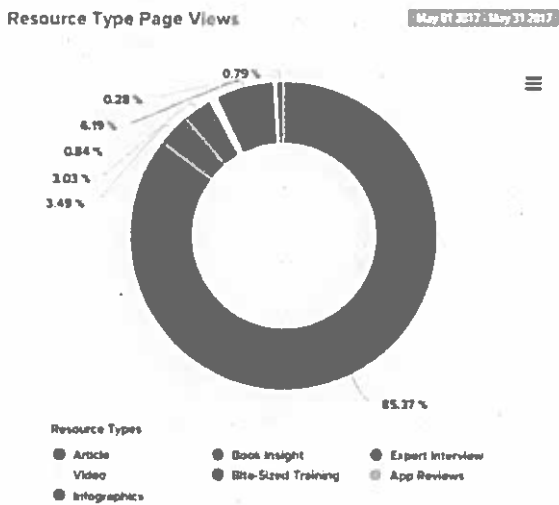
You can quickly change the date range on the homepage to view the data over your specified time period.

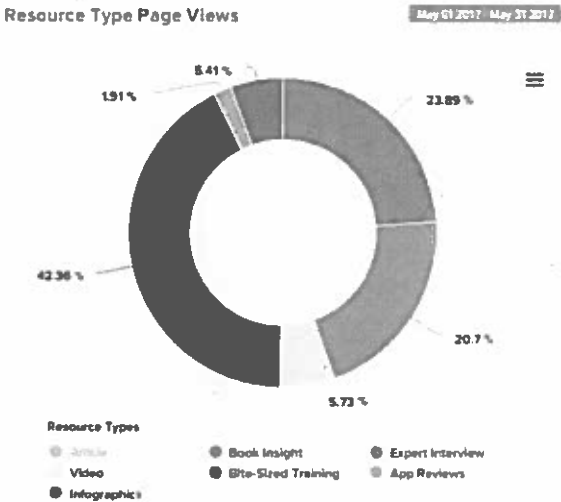


On each graph / chart / table use the additional menu for action points. This allows you to extract that piece of data which you can use to share with your team, add to presentations or use in other marketing or promotional activities.



On the front screen, click pieces of data you wish to hide. You can the assess the remaining data and interpret it without the hidden factor changing the results. You can do this with multiple factors at the same time.





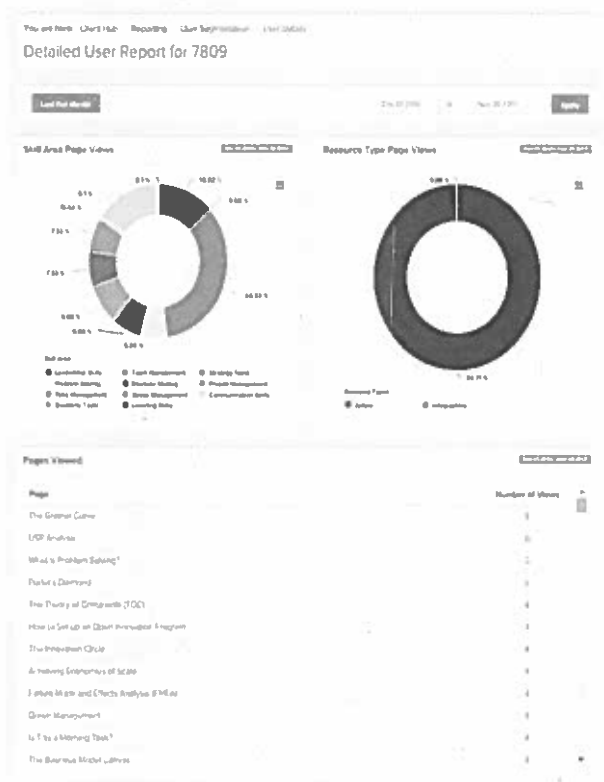
Within the Users vs Page View under the bottom section you will be able to click on the different users and then be able to see a list of what they are viewing as per the screenshots below:

User Page Views

Download CSV Download PDF

User	Page Views
7523	1021
5791	630
7449	564
8077	154
9633	112
7829	109
6124	108
7805	106
4275	99
5465	97
8093	93
8122	91

With the use of Unique Identifiers, we can also provide information on what each individual has viewed, as the below image illustrates.



Providing quality products

Each of the Mind Tools 2,000+ resources are researched and produced by our dedicated in-house editorial team and our professional writers and editors have 138 combined years of experience. Resources are based on the latest academic research, using credible sources and expert advice and are additionally supported by a blog archive of over 400 posts talking about learning in a professional setting.

All of our resources are housed within 12 'skill areas', the following images show these skill areas and list the sub-categories of tools and resources contained within each one.

Leadership Skills

Become an Exceptional Leader



Browse Tools by Category

Start Here (4)

General Leadership (5)

Understanding Power (2)

Leadership Styles (17)

Emotional Intelligence (16)

Becoming a Leader (7)

Young and Future Leaders (3)

Crisis and Contingency Planning (6)

▼

▼

▼

▼

▼

▼

▼

▼

Team Management

The Skills You Need to be a Great Boss

**409**
RESOURCES

Browse Tools by Category	
Start Here (12)	▼
Understanding Team Dynamics (17)	▼
Effective Recruitment and Induction (26)	▼
Developing Your Team (18)	▼
Coaching Your Team (20)	▼
Delegating Effectively (7)	▼
Motivating Your Team (16)	▼
Team Building Activities (7)	▼
Rewarding and Engaging Your Team (18)	▼
Improving Team Effectiveness (25)	▼
Performance Management (12)	▼
Difficult Management Situations (26)	▼
Managing Different Groups of Workers (49)	▼
Managing Different Types of Teams (10)	▼
Managing Around the World (41)	▼
Historical Management Theories (6)	▼

Strategy Tools

Mapping Out Your Best Possible Direction

240
RESOURCES

Browse Tools by Category

- Start Here (4)
- Core Strategy Tools (8)
- Competitive Advantage (17)
- Strategic Options (16)
- Organization Design (13)
- Strategic Prioritization (11)
- Executing Strategy (13)
- Sourcing and Purchasing Strategy (7)
- Marketing Strategy (30)
- Manufacturing and Operations (14)
- Quality Strategy (11)



Problem Solving

Solving Complex Business Problems

63
RESOURCES

Browse Tools by Category

- Start Here (3)
- General Problem-Solving Tools (6)
- Problem-Solving Approaches (15)
- Finding the Cause of a Problem (9)
- Improving Business Processes (11)
- Diagram-Based Tools (3)



Decision Making

How to Make Better Decisions



87
RESOURCES

Browse Tools by Category

Start Here (2)

Decision Making Models (6)

Choosing Between Options (9)

Deciding Whether to Go Ahead (9)

Financial Decisions (4)

Improving Decision Making (14)

The Impact of Ethics and Values (3)

Group Decision Making (9)

▼

▼

▼

▼

▼


▼

▼

▼

Project Management

Delivering Complex Projects Successfully



88
RESOURCES

Browse Tools by Category

Start Here (6)

Project Management Framework (14)

Scheduling (12)

Scope Management (4)

Communicating and Delegating (8)

Reporting Progress (2)

Change Management (14)

Project Improvement and Review (5)

▼

▼

▼

▼

▼

▼

▼

▼

40

Time Management

Beat Work Overload. Be More Effective. Achieve More.



106
RESOURCES

Browse Tools by Category

Start Here (4)

General Time Management Tools (11)

Prioritization (5)

Scheduling (4)

Time Management Challenges (8)

Concentration and Focus (9)

Goal Setting (14)

Self-Motivation (9)



Stress Management

Manage Stress. Be Happy and Effective at Work.



96
RESOURCES

Browse Tools by Category

Start Here (6)

Action-Based Strategies (5)

Perception-Based Strategies (10)

Coping Strategies (20)

Managing Performance Stress (4)

Happiness and Well-Being (11)

Relaxation and Sleep (5)

Self-Confidence and Self-Esteem (6)

Anger Management (3)

Burnout (5)



Communication Skills

Become a Skilled Business Communicator



232
RESOURCES

Browse Tools by Category

- Start Here (6)
- Planning and Structuring (16)
- Communicating in Person (23)
- Feedback (12)
- Meetings (18)
- Presentations (10)
- Communicating In Writing (18)
- Negotiation, Persuasion and Influence (20)
- Difficult Communication Situations (20)
- Understanding Others Better (7)



Creativity Tools

Develop Creative Solutions to Business Problems



55
RESOURCES

Browse Tools by Category

- Start Here (3)
- Brainstorming (9)
- Other Idea-Generation Tools (6)
- Creativity Processes (12)



Learning Skills

Learn – and Develop Others – More Effectively



64
RESOURCES

Browse Tools by Category

Personal Learning Skills (12)

Understanding How People Learn (15)

Developing a Learning Environment (10)

Reading More Effectively (7)

Memory Techniques (11)

▼

▼

▼

▼

▼

Career Skills

Thinking About Your Career...



329
RESOURCES

Browse Tools by Category

Thinking About Career Direction (13)

Understanding Your Strengths (6)

Career Tests (6)

Enhancing Your Job (6)

Effective Working Relationships (26)

General Career Skills (29)

Getting Ahead (20)

Getting a New Role (15)

Key Career Points (14)

Mentoring and Coaching (7)

Finance for Non-Specialists (8)

Understanding Different Sectors (8)

Understanding Culture (15)

Dealing with Challenges (24)

Dealing with Difficult People (12)

▼

▼

▼

▼

▼

▼

▼

▼

▼

▼

▼

▼

▼

▼

Provided in several resource types:

- **Articles** - often supported by short videos, articles are the bedrock of Mind Tools offering direct, simple information which can be instantly applied
- **Quizzes** - a fantastic way to start a learning journey, our quizzes give the learner a chance to get guidance on which areas (and therefore Mind Tools resources) are most important for them
- **Videos** - often supporting articles, our videos offer talking head guidance, simple montages and other fun ways to quickly get across a message (videos are between 2 and 5 minutes in length)
- **Podcasts** - supporting our book insights and expert interviews, podcasts are downloadable and perfect for commutes - between 15 and 35 minutes long
- **Infographics** - visualisation of ideas, great for a visual mindset and for group work, presents structures and frameworks with ease
- **Bite Sized Training** - downloadable workbooks to work through independently or as part of a team, great tool for team leaders and those with a passion for developing others
- **Templates and Worksheets** - downloadable worksheets to support activities - great for group work again and saves you time creating your own!
- **Learning Streams** - collections of tools you can work through to develop a particular skill e.g. Culture and Diversity. The closest thing we have to a training course!
- **App reviews** - great analysis and feedback on business applications that can help you, as a professional, progress in any of our focus areas
- **Scavenger Hunts** - activities used for driving engagement across the system - find answers to questions within the Mind Tools environment - complete the question to enter into a prize draw
- **Motivational Posters** - downloadable posters to be used across your office! You can even contact us to order them.

Accessed via your systems as well as on the move via the Mind Tools Corporate App:



Online individual self – assessment tools

To help the drive toward a self-directed continuous learning environment Mind Tools has created a set of 'Test Yourself' resources, again behind each of the 12 skill areas. These are designed to build self-awareness and help create for the individual user an acceptance of personal responsibility for their own learning.

The 'tests' themselves are easy to complete and are a great way of creating a double-positive effect, in this we mean based on the results (generated by the psychometrics that sit behind the tests) the individual quickly identifies what they are doing well in, but furthermore the output suggests additional resources for development and helps create that learner intrigue and want to learn.

The Test Yourself resources are easily accessed through the search functionality from what would be the CQC Mind Tools homepage or through the 'Other Resources' drop-down menu.

Test Yourself



Browse by Category

- Getting Started (5)
- Team Management (3)
- Leadership Skills (3)**

How Good Are Your Leadership Skills?

Find out how good your leadership skills are, where you could improve, and how you can move further along the path to effective leadership.

The Leadership Motivation Assessment

Take this self test to find out how motivated you are to lead. Then use your results to build on your leadership skills.

What's Your Leadership Style?

Use this quiz to find out how effective your usual approach to leading is, and to discover how you could improve.

After selecting the self-assessment resource, you are taken to an introductory paragraph that is often accompanied by a quick video followed by the assessment questions.

12 Statements to Answer		A	B	C
1	If there is serious conflict within my team: A. I remind everyone that we have goals to meet. B. I bring my people together so that we can talk it through. C. I let them work by themselves so that they don't have to bother one another.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	I trust my team members: A. Very much. B. A fair amount. C. Not at all.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	Some of my people are highly skilled and motivated. They: A. Can be set free to weave their magic. B. Often hold creative planning sessions with me. C. Are subject to the same workplace strategies and processes as everyone else.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4	The best way for me to ensure that my team meets its goals is to: A. Lead from the front. B. Encourage participation from everyone. C. Delegate often and widely.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5	We have an eight hour deadline for a project that I think requires 16 hours, so I: A. Relay the deadline and let everyone get on with it. They know what they're doing. B. Ask my team members what they feel is the fastest way to complete it. C. Issue instructions and deadlines to each team member.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6	Poor performance should be: A. Punished, so that it doesn't happen again. B. Talked through with the individual, so that we can learn. C. Left. It will work itself out.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7	I need to develop and apply a new social media strategy, so I: A. Draw up the strategy myself and then sell it to the team. B. Tell my team what the challenge is and ask for suggestions on how to meet it. C. Hand over the project to my team members and ask them to come back with a plan.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
8	I like to: A. Let my team make the decisions. B. Make a decision but not until my team has had input. C. Make a decision but not until I have told the team my rationale.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
9	I have a new starter in my team, so I: A. Let him discover the best way of working. B. Invite him into team collaborative meetings. C. Sit with him until he understands the processes and the quality that I expect.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
10	I think that great leaders: A. Know best. That's why they're leaders. B. Are humble and understand that a team works best collectively. C. Give their team members plenty of space to let them get on.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
11	When asked whether I like to serve my team, I: A. Am not sure. B. Say yes, wholeheartedly. C. Frown.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
12	I notice that a member of my team is demotivated, so I: A. Closely manage each of her tasks to ensure that she is following procedures correctly. B. Make an extra effort to ensure that she is involved in team discussions. C. Back off, as she probably needs some space.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

On completing the questions, the individual receives a score and a brief synopsis, however if they then click the 'Read Below' button or scroll down on the page they get a descriptive insight along with further resources to help them develop in those specific areas.

Score Interpretation

Score	Comment
12 20	<p>You most commonly adopt an authoritarian or autocratic leadership style. You rarely consult your team members and, instead, tend to tell them what you want, when you want it, and how you want it done.</p> <p>This style works well in a crisis, when a task must be completed quickly. However, you'll likely demoralize, demotivate and aggravate people if you use it all the time. This can translate into high absenteeism and turnover rates. You'll also miss out on a wealth of ideas, thereby stifling innovation and creativity. Read more below.</p>
21 27	<p>You lean toward a democratic or participative style of leadership. You tend to set the parameters for the work and have the final say on decisions, but you actively involve your team members in the process.</p> <p>This style can build trust between you and your people, as they'll likely feel engaged and valued. But it's not great in a high pressure situation that requires a fast turnaround, as it will slow you down. And, if you dislike disagreement or conflict, you might struggle with how people respond to consultation. Read more below.</p>
28 36	<p>Your default leadership style is probably delegating or "laissez faire." You give your team members free rein in how they work toward their goals.</p> <p>This is an ideal approach when your people are highly skilled and motivated, and when you're working with contractors and freelancers who you trust. But if a team member is inexperienced or untrustworthy, or if you lose sight of what's going on, this approach can backfire catastrophically. Read more below.</p>

Authoritarian, Autocratic Leadership

This approach is helpful when your team needs to follow a process "to the letter," to manage a significant risk. We also recommend being hands-on with employees who miss deadlines, in departments where conflict is an issue, or in teams that rely on quick decisions being made.

But you need to be aware that relying on control and punishment to maintain standards will drive people away, eventually. Similarly, if you always demand that your team works at top speed, you can end up exhausting everyone.

Instead, you can show respect for team members by providing the rationale for your decisions. And they will more likely comply with your expectations if you take the trouble to explain **Why the Rules Are There**.

You can improve your ability to "lead from the front" by **Planning for a Crisis**, **Thinking on Your Feet**, and **making good decisions under pressure**. But be sure to balance these skills with an awareness of their potential negative impact on creativity, ideas gathering, motivation, and trust within the team. Being too autocratic can also mean that you'll find it hard to stand back from the detail and take a wider, more strategic view.




Tip:

Did you achieve your leadership role thanks to your technical expertise? If so, you'll likely be used to getting things right, adding value, and having people's respect. But your soft skills might be lacking, so don't be afraid to listen and collaborate more.

The additional suggested resources for development can then be added to the individuals personal learning plan via the (+) icon or added directly to their calendar and into the flow of their work at a time to suit them:

The TDODAR Decision Model

Considering Your Options Under Pressure

Print 
Share 
Add to Calendar 



SCHEDULE 4 – PROCESSING, PERSONAL DATA AND DATA SUBJECTS

1. The contact details of the Controller's Data Protection Officer are: Nimali de Silva, Care Quality Commission, 3rd Floor, Buckingham Palace Road, London SW1W 9SZ.
2. The contact details of the Processor's Data Protection Officer are: Ollie Craddock, ollie.craddock@mindtools.com
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 13.1.
Subject matter of the processing	Mind Tools processes personal data in relation to employees and other individuals who have been given access to the service by the customer.
Duration of the processing	The duration of the contract including any agreed extensions.
Nature and purposes of the processing	<p>Personal Data is processed by Mind Tools for the following purposes:</p> <ul style="list-style-type: none"> • To administer Mind Tools' site and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes. • To improve Mind Tools' site to ensure that content is presented in the most effective manner for the User and their device. • To allow the User to participate in interactive features of Mind Tools' service, when they choose to do so. • As part of Mind Tools efforts to keep its site safe and secure. • To make suggestions and

	<p>recommendations to Users of Mind Tools' site about content and features that may interest them.</p> <ul style="list-style-type: none"> • To communicate relevant Mind Tools resources to individual Users. • To provide reporting data to the customer of usage of the resources by the Users
<p>Categories of Personal Data</p>	<p>The categories of Personal Data processed by Mind Tools comprise:</p> <ul style="list-style-type: none"> • Customer generated User ID (Unique Identifier). • MT generated User ID (will be the same as customer generated ID if provided). • Email address of the User (if provided with consent). • First name of the User (if provided with consent). • Personal information from the User to identify their learning needs - for example job role, seniority, skills gaps. • Technical information, including the Internet protocol (IP) address used to connect the User's computer to the Internet, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform. • Information about the User's visit, including the full Uniform Resource Locators (URL) clickstream to, through and from our Website (including date and time); page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), methods used to browse away from the page. • Cookies: Mind Tools' website uses cookies to distinguish the User from other Users of our website. This helps Mind Tools to provide the User with a good experience when the User browses Mind Tools' website and also allows Mind Tools to improve its site.

Categories of Data Subject	Users who have been given access to the service by the customer.
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	All user data provided by the CQC will be destroyed upon completion of the contract. Any user data created by the contractor will be provided to the CQC who will store and destroy in accord with CQC retention policy and procedures.

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

[Refer to Annex 2]

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

Mind Tools Access Control Policies

Revision History

Ver	Date	Author	Description	Comments
1.0	18/08/2016	GP	First draft	
1.1	15/08/2018	GD	Update post GDPR	

Audience

This policy applies to all Mind Tools staff who have responsibility for computing devices.

Compliance

Failure to comply with this policy may put Mind Tools assets at risk and may have disciplinary consequences for employees. Violation of this policy may also carry the risk of criminal penalties.

1. Policy Statement

1.1. Protecting access to IT systems and applications is critical to maintain the integrity of the Mind Tools technology and data and prevent unauthorised access to such resources.

1.2. Access to Mind Tools systems must be restricted to only authorized users or processes, based on the principle of strict need to know and least privilege.

2. Background

2.1. Access controls are necessary to ensure only authorized users can obtain access to Mind Tools' information and systems.

2.2. Access controls manage the admittance of users to system and network resources by granting users access only to the specific resources they require to complete their job related duties.

3. Policy Objective

3.1. The objective of this policy is to ensure Mind Tools has adequate controls to restrict access to systems and data.

4. Passwords

4.1. Each user should have a unique username and password

4.2. Passwords must be high strength and where possible be:

- a. Minimum of 8 characters
- b. At least three of the following characteristics
 - i. Contains lower case letters
 - ii. Contains upper case letters
 - iii. Contains numbers
 - iv. Contains non-alphanumeric characters
- c. Not easily guessed, for example containing personal information, pet names, family details etc.

4.3. Users are not permitted to share their username or password with anyone, including other Mind Tools staff

4.4. Two factor authentication is to be used where possible

5. Password Storage

5.1. Passwords should never be written down

5.2. The Mind Tools official way of storing passwords is using the Keeppass software

6. Workstation security

6.1. All computers should be secured with an automatic locking system that requires a password to unlock. The delay before auto locking should not exceed 1 hour

6.2. All computers should have encryption enabled on the disk

6.3. All computers are to have firewall software installed and enabled

6.4. All computers are to use up to date Anti Virus software (with exception of OSX and Linux which are deemed low risk)

7. Remote Access

7.1. Rackspace / Cisco VPN software is to be used for connecting to company servers (See Remote Access Policy)

8. Wireless Access

8.1. Encryption must be enabled

9. System Access

9.1. Mind Tools will provide access privileges to technology (including networks, systems, applications, computers and mobile devices) based on the following principles:

9.1.1. Need to know – users or resources will be granted access to systems that are necessary to fulfill their roles and responsibilities.

9.1.2. Least privilege – users or resources will be provided with the minimum privileges necessary to fulfill their roles and responsibilities.

9.2. Application and service accounts must only be used by application components requiring authentication; access to the passwords must be restricted to authorized IT administrators or application developers only.

9.3. Where possible, the Institution will set user accounts to automatically expire at a pre-set date. More specifically,

9.3.1. When temporary access is required, such access will be removed immediately after the user has completed the task for which the access was granted.

9.3.2. User accounts assigned to contractors will be set to expire according to the contract's expiry date.

9.4. Access rights will be immediately disabled or removed when the user is terminated or ceases to have a legitimate reason to access Mind Tools systems.

9.5. Existing user accounts and access rights will be reviewed at least biannually to detect dormant accounts and accounts with excessive privileges.

Information Protection Policy

Mind Tools Ltd.

17 August 2016

Category Information Security

Version 1.0

Classification Public

Document Control

Organisation	Mind Tools Ltd.
Title	
Author	
Filename	
Owner	
Subject	IT Policy
Protective Marking	[Marking Classification]
Review date	17/01/20

Revision History

Revision Date	Version Number	Revised By	Description of Revision
17 Aug 2016	1.0		First version of ISP doc
17 Jan 2019	1.1		First full revision

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address / Location

Table of Contents

Policy Statement

Purpose

Scope

Definition

Risks

Applying the Policy

Policy Compliance

Policy Governance

Review and Revision

References

Key Messages

Appendix 1

A1 Applying the Policy

A1.1 Information Asset Management

A1.1.1 Identifying Information Assets

A1.1.2 Assigning Asset Owners

A1.1.3 Unclassified Information Assets

A1.1.4 Information Assets with Short Term or Localised Use

A1.1.5 Corporate Information Assets

A1.1.6 Acceptable Use of Information Assets

A1.2 Information Storage

A1.3 Disclosure of Information

Policy Statement

Mind Tools will ensure the protection of all information assets within the custody of the Business.

High standards of confidentiality, integrity and availability of information will be maintained at all times.

Purpose

Information is a major asset that Mind Tools Ltd. has a responsibility and requirement to protect.

Protecting information assets is not simply limited to covering the stocks of information (electronic data or paper records) that the Organisation maintains. It also addresses the people that use them, the processes they follow and the physical computer equipment used to access them.

This Information Protection Policy addresses all these areas to ensure that high confidentiality, quality and availability standards of information are maintained.

The following policy details the basic requirements and responsibilities for the proper management of information assets at Mind Tools Ltd. The policy specifies the means of information handling and transfer within the Business.

Scope

This Information Security Policy applies to all the systems, people and business processes that make up the Business's information systems. This includes all Executives, Committees, Departments, Partners, Employees, contractual third parties and agents of the Organisation who have access to Information Systems or information used for Mind Tools Ltd. purposes.

Definition

This policy should be applied whenever Business Information Systems or information is used. Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper.
- Data stored electronically.
- Communications sent by post / courier or using electronic means.
- Stored tape or video.
- Speech.

Risks

Mind Tools Ltd. recognises that there are risks associated with users accessing and handling information in order to conduct official business.

This policy aims to mitigate the following risks:

- Non-reporting of information security incidents
- Inadequate destruction of data in electronic and non-electronic format
- The loss of direct control of user access to information systems

Non-compliance with this policy could have a significant effect on the efficient operation of the organisation and may result in financial loss and an inability to provide necessary services to our customers.

Applying the Policy

For information on how to apply this policy, readers are advised to refer to Appendix 1.

Policy Compliance

If any user is found to have breached this policy, they may be subject to Mind Tools disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Development Team.

Policy Governance

The following table identifies who within Mind Tools Ltd. is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible		
Accountable		
Consulted		
Informed		

Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the Senior Development Manager.

References

The following Mind Tools Ltd. policies and guidelines are directly relevant to this policy, and are referenced within this document

- Email, Computer, Telephone and Internet Usage Policy (Employee Handbook 3.11)
- Data Retention Policy
- Homeworking Policy. (Employee Handbook 3.18)
- Access Control Policy
- Personal Data Breach Policy

Key Messages

- The Business must draw up and maintain inventories of all important information assets.
- All information assets, where appropriate, must be assessed and classified by the owner in accordance with the Mind Tools Ltd Security Policy (SPF).
- Access to information assets, systems and services must be conditional on acceptance of the Email, Computer and Internet Usage Guidelines (Employee Handbook).
- Users should not be allowed to access information until the Senior Development Manager is satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.
- Mind Tools information must not be disclosed to any other person or organisation via any insecure methods including paper based methods, fax and telephone.
- Disclosing Mind Tools classified information to any external organisation is also prohibited, unless formal permission has been granted.
- The disclosure of Mind Tools classified information, without explicit permission in any way is a disciplinary offence.

Appendix 1

A1 Applying the Policy

A1.1 Information Asset Management

A1.1.1 Identifying Information Assets

The process of identifying important information assets should be sensible and pragmatic.

Important information assets will include, but are not limited to, the following:

- Filing cabinets and stores containing paper records.
- Computer databases.
- Data files and folders.
- Software licenses.
- Physical assets (computer equipment and accessories, PDAs, cell phones).
- Key services.
- Key people.
- Intangible assets such as reputation and brand.

Mind Tools Ltd. must draw up and maintain inventories of all important information assets that it relies upon. These should identify each asset and all associated data required for risk assessment, information/records management and disaster recovery. At minimum it must include the following:

- Type.
- Location.
- Designated owner.
- Security classification.
- Format.
- Backup.
- Licensing information.

Personal Information

Personal information is any information about any living, identifiable individual. The business is legally responsible for it. Its storage, protection and use are governed by the Data Protection Act 1998 and General Data Protection Regulation 2018. Details of specific requirements can be found in the Data Retention Policy.

A1.1.2 Assigning Asset Owners

All important information assets must have a nominated owner and should be accounted for. An owner must be a member of staff whose seniority is appropriate for the value of the asset they own. The owner's responsibility for the asset and the requirement for them to maintain it should be formalised and agreed.

A1.1.3Unclassified Information Assets

Items of information that have no security classification and are of limited or no practical value should not be assigned a formal owner or inventoried. Information should be destroyed if there is no legal or operational need to keep it and temporary owners should be assigned within each department to ensure that this is done. The procedure for destroying information can be accessed in the Data Retention Policy.

A1.1.4Information Assets with Short Term or Localised Use

For new documents that have a specific, short term localised use, the creator of the document will be the originator. This includes letters, spreadsheets and reports created by staff. All staff must be informed of their responsibility for the documents they create.

A1.1.5Corporate Information Assets

For information assets whose use throughout the organisation is widespread and whose origination is as a result of a group or strategic decision, a corporate owner must be designated and the responsibility clearly documented. This should be the person who has the most control over the information.

A1.1.6Acceptable Use of Information Assets (Employee Handbook)

Mind Tools make available (in the Employee Handbook) guidelines on acceptable use for information assets, systems and services. These guidelines should apply to all Mind Tools Ltd. Executives, Committees, Departments, Partners, Employees, contractual third parties and agents of the business and use of the system must be conditional on acceptance of the appropriate guidelines.

As a minimum this will include:

- Email, Computer and Internet Usage Policy (including Removable Media) (Employee Handbook 3.11)
- Remote Working Policy. (Employee Handbook 3.18)

A1.2 Information Storage

All electronic information will be stored on centralised facilities to allow regular backups to take place.

Staff should not be allowed to access information until their line manager is satisfied that they understand and agree the legislated responsibilities for the information that they will be handling.

Databases holding personal information will have a defined security and system management procedure for the records and documentation.

This documentation will include a clear statement as to the use, or planned use of the personal information.

Files which are identified as a potential security risk should only be stored on secure network areas e.g. Production Database Servers.

A1.3 Disclosure of Information

A1.3.1 Sharing Mind Tools Information with other Organisations

Mind Tools information **must not** be disclosed to any other person or organisation via any insecure method including, but not limited, to the following:

- Paper based methods.
- Fax.
- Telephone.

Where information is disclosed/shared it should only be done so with explicit authorisation from your line manager.

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	£
	Contract Change Note [x]	£
	New Contract Value	£
Revised Payment Schedule		
Revised Specification (See Annex [x] for Details)		
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 determined with supplier at the kick off meeting]