EDULINCS

GENERAL TERMS AND CONDITIONS

Schedule 1

PART 1: SERVICE SPECIFIC CONDITIONS

1. Renewal

Not applicable.

2. Termination Period

The termination period for these services is 30 days from the date of the Order Form being signed by the Client.

3. Charges for these Services are

Option	Schools with 100+ pupils	Schools with fewer than 100 pupils*
Document package (one off)	£399	£319
Advice package (annual cost)	£699	£559
Document and advice package (annual cost)	£999	£799
Freedom of Information bolt-on	£249	£199
Ad-Hoc Service (fixed hourly rate)	£65	£52
*20 per cent discount for schools with fewer than 100 pupils		

4. GDPR relationship for the Service is:

Data Controllers, independent of one another, as set out in the relevant sections of Part 2 of this Schedule.

5. Invoicing details for the Service are as follows:

Services will be invoiced by the relevant October half term (any outstanding invoices to be completed in the following half term).

6. Specific Service conditions

Not applicable.

PART 2: PROCESSING, PERSONAL DATA AND DATA SUBJECTS

SECTION A

Definitions:

Client's Personal Data means the Personal Data supplied by the Client to the Council and/or Personal Data collected by the Council on behalf of the Client for the purposes of or in connection with the Agreement.

Controller takes the meaning given in the UK GDPR.

Data Protection Legislation means (i) the UK GDPR; (ii) the DPA to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy.

Data Protection Impact Assessment means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

Data Protection Officer takes the meaning given in the UK GDPR.

Data Loss Event means any event that results, or may result, in unauthorised access to Personal Data held by the Council under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

Data Subject takes the meaning given in the UK GDPR.

Data Subject Request means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation.

DPA means the Data Protection Act 2018.

ICT means information and communications technology.

ICT Environment means the Client's system and the Council system.

Information has the meaning given under section 84 of the FOIA and includes Personal data as defined under Data Protection Legislation.

Information Commissioner's Office means the office of the Information Commissioner whose role is to uphold information rights in the public interest, and responsible for data protection in England, Scotland and Wales in accordance with provisions set out in the DPA.
Joint Controllers means where two or more Controllers jointly determine the purpose and means of processing.

Personal Data takes the meaning given in the UK GDPR.

Personal Data Breach takes the meaning given in the UK GDPR.

Processing takes the meaning given in the UK GDPR.

Processor takes the meaning given in the UK GDPR.

Protective Measures means appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it including those outlined in Part 2 of Schedule 1.

Sub-processor means any third party appointed to process Personal Data on behalf of the Council related to this Agreement.

SECTION B

1. The Parties are each Controllers, independent of one another and are separately responsible for meeting their respective obligations under Data Protection Legislation.

2. The Supplier shall comply with the data processing provisions set out in Section C of this Schedule 1.

SECTION C

The point of contact for Data Subjects is: Amy Jaines, Data Protection Officer, Lincolnshire County Council, or her successor.

Description	Details
Identity of the Client and the Council	The parties acknowledge that for the purposes of the Data Protection Legislation, the client and the supplier are Controllers independent of each other.
Subject matter of the processing	The processing is needed in order to ensure that the Council can effectively deliver the Agreement. The Council will provide the Client with a Data Protection Advice Service.
Duration of the processing	Duration of the Agreement.
Nature and purposes of the processing	The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means). The purpose of the processing of Personal Data is to enable the provision of public services which includes: • Providing advice and guidance on the Data Protection Legislation • Assisting with handling and responding to individual rights requests • Assisting with handling and responding to personal data breaches
Type of Personal Data	The type of Personal Data which is Processed under this Agreement may include: • Personal details e.g. name, address, date of birth, pupil or NI number, telephone number; • family detail e.g. personal details of relatives, legal guardians and friends; • lifestyle and social circumstances e.g. physical or mental health details, racial or ethnic origin, trade union membership, offences (including alleged offences), religious or other beliefs of a similar nature; • employment and education details; • student and pupil records; • safeguarding information; • business activities; • case file information.

Categories of Data Subject	Categories of Data Subject may include: • staff and governors • students and pupils • parents, carers, representatives or legal guardians • other professionals
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	As independent controllers, each controller shall retain their own records for as long as necessary in accordance with their own defined periods of retention.

SECTION D - MINIMUM INFORMATION SECURITY CONTROLS

The minimum security controls detailed within this Part 2 of Schedule 1 are to be in place at all times when processing Information for the purpose of or in connection with the delivery of the Services. Such Information includes Personal Data and other Confidential Information or data.

1. GENERAL

1.1 Both Parties shall have a security policy in place which sets out management commitment to information security, defines information security responsibilities, and ensures appropriate governance.

1.2 All Staff shall complete data protection and information security training commensurate with their role.

2. ICT INFRASTRUCTURE

Boundary Firewall and Internet Gateways

2.1 Information, applications and devices shall be protected against unauthorised access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices.

Secure Configuration

2.2 ICT systems and devices shall be configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.

User Access Control

2.3 User accounts shall be assigned to authorised individuals only, managed effectively, and they shall provide the minimum level of access to applications, devices, networks, and Personal Data.

2.4 Access control (username & password) shall be in place. A password policy shall be in place which includes provisions to ensure:-

(a) avoidance of the use of weak or predictable passwords;
(b) all default passwords are changed;
(c) robust measures are in place to protect administrator passwords; and
(d) account lock out or throttling is in place to defend against automated guessing attacks.

2.5 End user activity shall be auditable and include the identity of end-users who have accessed systems.

Malware Protection

2.6 Mechanisms to identify detect and respond to malware on ICT systems and devices shall be in place and shall be fully licensed, supported, and have all available updates applied.

Patch Management and Vulnerability Assessment

2.7 Updates and software patches shall be applied in a controlled and timely manner and shall be supported by patch management policies.

2.8 The Council shall adopt a method for gaining assurance in its organisation's vulnerability assessment and management processes, for example by undertaking regular penetration tests.

2.9 Software which is no longer supported shall be removed from ICT systems and devices.

Cloud Services

2.10 The Council shall ensure that the controls applied to the use of cloud services satisfactorily support the relevant security principles set out in the National Cyber Security Centre Cloud Security Principles:
https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

3. PROTECTING INFORMATION

Electronic Information

3.1 Electronic copies of Information shall be encrypted at rest to protect against unauthorised access.

3.2 When transmitting Information over the internet, over a wireless communication network e.g. Wi-Fi, or over an untrusted network the Parties shall use an encrypted communication protocol.

3.3 The Parties shall only use ICT, which is under its governance and subject to the controls set out in this Schedule.

Hard Copy Confidential Information

3.4 Hard copy Confidential Information shall be stored securely when not in use and access to it shall be controlled.

3.5 Hard copy Confidential Information shall be transported in a secure manner commensurate with the impact a compromise or loss of information would have, and which reduces the risk of loss or theft.

Secure Destruction of Information

3.6 Electronic copies of Information shall be securely destroyed when no longer required, including Information stored on servers, desktops, laptops or other hardware and media.

3.7 Hard copy Information shall be securely destroyed when no longer required.

3.8 Secure destruction means destroying Information so it cannot be recovered or reconstituted.

3.9 A destruction certificate may be required by the Client to provide the necessary assurance that secure destruction has occurred.

4. COMPLIANCE

4.1 Each Party shall inform the other of any non-compliance with the controls set out in this Schedule. Any deficiencies in controls shall be subject to a documented risk management process and where appropriate a remediation plan shall be implemented with the aim of reducing, where possible, those deficiencies.

4.2 Independent validation which has been used as evidence of appropriate security controls by each Party shall be maintained by each Party for the duration of the Agreement.

4.3 Each Party shall inform the other of any expired or revoked evidence used as independent validation.