EDULINCS

GENERAL TERMS AND CONDITIONS

Schedule 1

PART 1: SERVICE SPECIFIC CONDITIONS

1. Renewal

a) Automatic renewal does not apply to this Service. Where the Client wishes to continue receiving the Services for the next academic year, the Client must reorder at the beginning of each academic year by completing and submitting the necessary forms, as the Council directs.

b) Subject 1(c) and (d) below, a standard renewal fee (as set out on the Edulincs page: https://www.lincolnshire.gov.uk/directory-record/66287/clerking) ("EduLincs Page")) shall be payable when the Services are renewed.

- Renewal 1 will cover the following:
    - Pre-Governor hub maintenance and specific work for the Client.
    - Administration work to set up the Client for the new academic year.
    - Governorhub One Subscription.
    - Teams Premium Subscription.
- Renewal 2 will cover the following:
    - Pre-Governor hub maintenance and specific work for the Client.
    - Administration work to set up the Client for the new academic year.
    - Teams Premium Subscription.

d) A special renewal fee will apply for maintained school settings who require constitutional changes (e.g. federation of schools). The following year, if there are no further changes to the constitution, this will revert back to the standard renewal fee. Fees are as per the EduLincs Page.

e) A special renewal fee will apply for any multi academy trusts who require amalgamation of Local Governing Boards / Academy Committees. The following year, if there are no further changes to the constitution, this will revert back to the standard renewal fee. Fees are as per the EduLincs Page.

2. Termination

a) Within 14 calendar days of the Client accepting the Council's quotation for the provision of Services, the Client may terminate this Agreement for any reason with immediate effect upon the Council receiving written notice from the Client confirming the same within those 14 calendar days. In such circumstances the Client shall not be liable to pay any cancellation charges, however the Client shall pay for any Services rendered up until the date of termination. Any joining fee that has been paid will be reimbursed to the Client by the Council.

b) After the first 14 calendar days of the Client accepting the Council's quotation for the provision of Services, the Client may terminate this Agreement for any reason upon giving the Council written notice of the same, with such notice period ending at the end of the academic term (winter, spring or summer) within which the notice has been served. The Client shall be liable to pay all Charges in respect of the Services until the end of the notice period.

c) The Council may terminate this Agreement for any reason at any time upon giving the Client 30 calendar days' written notice, or such longer period as the notice may specify.

3. Charges for this Service

a) The Charges vary depending on the Services required and will be agreed between the Council and the Client, as set out in (or calculated in accordance with) the Order Form.

b) A joining fee (as per the EduLincs Page) shall be payable where the Client is a new recipient of the Services.

4. Data Protection

The Client is the Data Controller, and the Council is the Data Processor, and the Parties shall comply with the terms set out in Part 2 of this Schedule 1.

5. Invoicing

The Council shall issue invoices in accordance with the following schedule:

a) September to March – invoice will be sent between September and November
b) April to August – invoice will be sent in April.
c) Any additional meetings or extra work will be charged separately and invoiced quarterly in arrears (December, March, June, August).

6. Council Retention Process

a) As part of the Council's role in providing the Services, it shall retain copies of the Client's governance records (including but not limited to meeting minutes, agendas, governing body member information, details of any complaints) ("Governance Records") until such time as detailed at 6(b) and (c) below. The Clerk shall send to the Client a copy of all Governance Records that are not available in Governorhub (i.e. HR documents, PEX, PDC, HT Recruitment, Complaints etc) that they have received or created during the relevant academic year via email at the end of each academic year. It is the Client's decision of how and where to receive these documents. The Clerk shall also add these documents to Governor hub where possible. **Once received, the Client must apply their own retention policy to these documents.**

b) Subject to 6(c), although the Governance Records are owned by the Client the Council shall retain a copy of the same for **two years** after they have been sent to the Client at the end of an academic year in accordance with 6(a), for reference to provide administrative support. After the two years have elapsed, the Council shall securely destroy the relevant Governance Record.

c) Upon expiry or termination of this Agreement, the Clerk shall send all Governance Records *(that are not in Governor Hub)* received or created in the current academic year when termination or expiry occurs to the Client. Once the Client has confirmed in writing receipt of the same, the Council shall securely destroy all Governance Records held within 30 calendar days of such confirmation.

7. The Services

a) The Council will:
- Provide an independent, trained substantive clerk to Governors, appointed specifically to your governing body (referred to from this point forward as "the Clerk"). Allocation of

the Clerk may be subject to review if the Council identifies that the needs of the Client's governing body and/or the Service have changed.

- Provide a replacement Clerk at no extra cost if the Clerk cannot attend.
- Calculate the Charges of the Service based on the number of meetings specified in the Order Form.
- Arrange an introductory meeting, in person or virtually, between the Council's Business Support Service Manager / Senior Business Support Assistant, the Clerk (if in position), the Chair of Governors and the Headteacher.
- Undertake all line management of Business Support staff, including training and appraisals, liaising with the Client and/or Chair of Governors as and when appropriate.
- Provide a centralised governance IT system for your governing body when appropriate, within which data will be updated by the Council's School Support Team and the Clerk; and
- Provide IT equipment for the Clerk and ensure that they have access to secure email and governance IT system, along with the means to hold meetings virtually.

b) The Client will:

- Provide the Council (Business Support team) with a named primary point of contact.
- Inform the Council of the number of Governor's meetings anticipated for the academic year and the usual day/time these would take place. These must be subject to change to ensure clerk availability.
- Maintain regular communication with the Clerk.
- Raise any issues concerning performance or attendance with the Council's Business Support Service Manager.
- Provide 2 weeks' notice to the Clerk and Council's School Support Team prior to cancellation or rearrangement of any meeting.
- Ensure all invoices are paid within 30 days of receipt.
- Provide the Clerk with a list of current Governors, their email addresses and telephone numbers, their current Board responsibilities, and their dates of appointment.
- Provide the Clerk with a copy of the Governing Body paperwork – including, but not limited to the following:
    - previous agendas.
    - minutes.
    - terms of reference.
    - scheme of delegation.
    - governor induction paperwork.
    - policy schedule.
    - Governing body Disclosure and Barring Service details.
    - Section 128 Education and Skills Act 2008 information; and
    - School Improvement/Development Plan.

c) Both Parties will:

- notify the other Party in writing at the earliest opportunity should there be any changes to the named primary contacts.
- understand that this agreement will give schools the opportunity to sign a Memorandum of Understanding to utilise governors from other school governing bodies if necessary/appropriate to ensure that panels are convened effectively and efficiently.
- ensure that all correspondence is sent securely; and
- work together within local and national guidance and support each other to identify any concerns.

d) The Clerk is and shall remain an employee of the Council at all times. The Client shall not directly or indirectly employ or engage any services from the Clerk. If the Client breaches this condition they shall pay a compensation fee, which the Council shall confirm to the Client in writing. The Council shall calculate such compensation fee as a genuine pre-estimate of the financial loss the Council would incur in recruiting and training a new staff member.

e) Where the Client cancels a meeting, and such notice of cancellation is given to the Council 2 or more weeks' notice before the meeting is due to take place, the Client shall be reimbursed for the Charge for that meeting and the financial adjustment shall be applied to the next invoice.

f) Where the Client cancels a meeting, and such notice of cancellation is given to the Council less than 2 weeks' before the meeting is due to take place, the Client shall be liable to pay the following:

   i. Cancel 3 or more days before the meeting: 25% of the Charge for the meeting.
   ii. Cancel the day before or the same day of the meeting: 50% of the Charge for the meeting.

   and a financial adjustment shall be applied to the next invoice. However, the Council may, in its absolute discretion, waive the above cancellation charges upon taking the reasons for cancellation, plus any mitigating circumstances, into account.

g) If virtual or hybrid support is provided by the Clerk, the Council will provide a specific IT device to enhance the acoustics of the meeting. This IT device will be provided free of charge. This device will only be provided to the Client if all the yearly meetings are supported by the Clerk virtually or on a hybrid basis, or the Clerk only attends only 1 or 2 face to face meetings a year. The IT device shall be returned to the Council within 30 calendar days following expiry or termination of the Agreement. If the Client fails to return the item, they shall be liable to pay a charge of £30 to the Council.

h) The Council's School Support Team communicates messages with schools via a range of methods. This includes a newsletter about the Service and the School Support Service in general, as well as other relevant updates, delivered via third party system called 'Mailchimp'. If the Client would prefer not to receive this, they can opt out via written request to BS_SchoolSupport@lincolnshire.gov.uk.

PART 2: PROCESSING, PERSONAL DATA AND DATA SUBJECTS

SECTION A

Definitions:

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.

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 acknowledge that for the purposes of the Data Protection Legislation, the Client is the Controller, and the Council is the Processor. The only processing that the Council is authorised to do is listed in this part 2 of Schedule 1 by the Client and may not be determined by the Council.

2. The Council shall notify the Client immediately if it considers that any of the Client's instructions infringe the Data Protection Legislation.

3. The Council shall provide all reasonable assistance to the Client in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Client, include: -

(a) a systemic description of the envisaged processing operations and the purpose of the processing.

(b) an assessment of the necessity and proportionality of the processing operations in relation to the Services.

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

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

4. The Council shall, in relation to any Personal Data processed in connection with its obligations under this Agreement: -

(a) process that Personal Data only in accordance with part 2 of Schedule 1, unless the Council is required to do otherwise by Law. If it is so required, the Council shall promptly notify the Client 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 Client may reasonably reject (but failure to reject shall not amount to Approval by the Client 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 Staff do not process Personal Data except in accordance with this Agreement (and in particular part 2 of Schedule 1).

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

(A) are aware of and comply with the Council's duties under this clause.

(B) are subject to appropriate confidentiality undertakings with the Council 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 Client or otherwise permitted by this Agreement; and

(D) have undergone adequate training in the use, care, protection, and handling of Personal Data.

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

(i) the Client or the Council has provided appropriate safeguards in relation to the transfer as determined by the Client.

(ii) the Data Subject has enforceable rights and effective legal remedies.

(iii) the Council 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 all reasonable endeavours to assist the Client in meeting its obligations); and

(iv) the Council complies with any reasonable instructions notified to it in advance by the Client with respect to the processing of the Personal Data.

(e) at the written direction of the Client, delete or return Personal Data (and any copies of it) to the Client on termination of the Agreement unless the Council is required by Law to retain the Personal Data.

5. Subject to paragraph 6, the Council shall notify the Client 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's Office or any other regulatory authority in connection with Personal Data processed under this Agreement.

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

(f) becomes aware of a Data Loss Event.

6. The Council's obligation to notify under paragraph 5 shall include the provision of further information to the Client in phases, as details become available.

7. Taking into account the nature of the processing, the Council shall provide the Client with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 5 (and insofar as possible within the timescales reasonably required by the Client) including by promptly providing:-

(a) the Client with full details and copies of the complaint, communication, or request.

(b) such assistance as is reasonably requested by the Client to enable the Client to comply

with a Data Subject Request within the relevant timescales set out in the relevant Data Protection Legislation.

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

(d) assistance as requested by the Client following a Data Loss Event.

(e) assistance as requested by the Client with respect to any request from the Information Commissioner's Office, or any consultation by the Client with the Information Commissioner's Office.

8. The Council shall maintain complete and accurate records and information to demonstrate its compliance with this part A. This requirement does not apply where the Council employs fewer than 250 staff, unless the Client determines: -

(a) that the processing is not occasional.

(b) the processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

(c) the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

9. The Council shall allow for audits of its Processing activity by the Client or the Client's designated auditor.

10. Each Party shall designate its own Data Protection Officer if required by the Data Protection Legislation.

11. Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Council shall: -

(a) notify the Client in writing of the intended Sub-processor and Processing.

(b) obtain the written consent of the Client.

(c) enter into a written agreement with the Sub-processor which gives effect to the terms set out in this part A such that they apply to the Sub-processor; and

(d) provide the Client with such information regarding the Sub-processor as the Client may require.

12. The Council shall remain fully liable for all acts or omissions of any Sub-processor.

13. The Council may, at any time on not less than thirty (30) Working Days' notice, revise this section A by replacing it with any applicable Controller to Processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).

14. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Council may on not less than thirty (30) Working Days' notice to the Client amend this Agreement to ensure that it complies with any guidance issued by the Information

Commissioner's Office.

15. The Council acknowledges that, in the event that it breaches (or attempts or threatens to breach) its obligations relating to Personal Data, the Client may be irreparably harmed (including harm to its reputation). In such circumstances, the Client may proceed directly to court and seek injunctive or other equitable relief to remedy or prevent any further breach (or attempted or threatened breach).

16. In the event that through failure by the Council to comply with its obligations under the Agreement, the Personal Data is transmitted or Processed in connection with the Agreement is either lost or sufficiently degraded so as to be unusable, the Council shall be liable for the cost of reconstitution of that data and shall reimburse the Client in respect of any charge levied for its transmission and any other costs charged in connection with such failure by the Council.

17. The provision of this part A shall apply for the duration of the Agreement and indefinitely after its expiry.

SECTION C

1. The Council shall comply with the instructions of the Client with respect to processing as set out in this Schedule 1.

2. The Council shall comply with any further written instructions with respect to processing by the Customer.

3. Any such further instructions shall be deemed to be incorporated into this Schedule as if originally forming part thereof.
4. 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 is the Controller, and the Council is the Processor.
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 clerking 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: • A clerking service, to schools

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.
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	Upon termination or expiry of the contact all Personal Data shall be returned to the Client, unless instructed otherwise. If the Client does not request the Personal Data to be returned, then it shall be deleted or destroyed within six (6) months and the Council shall confirm in writing that the data has been securely deleted or destroyed.

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 supports 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.