EDULINCS

GENERAL TERMS AND CONDITIONS

Schedule 1

PART 1: SERVICE SPECIFIC CONDITIONS

1. Renewal

Automatic renewal does not apply to this Service. Where the Client wishes to continue receiving the Services for a further twelve (12) months, the Client must reorder by completing and submitting the necessary forms, as the Council directs. The Client may place an order for the Services at any time during an academic year.

2. Termination

Either party may terminate this Agreement for any reason at any time upon giving the other 30 calendar days' written notice, or such longer period as the notice may specify. No refunds or part refunds shall be given in the event of termination by the Client.

3. Charges

The Charges for this Service are as follows:

- annual Governorhub One subscription Band 1 (0–100 pupils): **£500**
- annual Governorhub One subscription Band 2 (101–400 pupils): **£595**
- annual Governorhub One subscription Band 3 (401–600 pupils): **£650**
- annual Governorhub One subscription Band 4 (601 – 999 Pupils): **£695**
- Multi Academy Trust: £525 trust board and £595 per additional local governing board
- Gov Hub Training Package**:** Online Training sessions with questions and feedback (support included)
    - Training session **£195**
    - Training session and refresher **£250** (when needed through the Academic Year)

4. Data Protection

a) The Parties do not envisage the processing of any Personal Data* as part of this Agreement.

*Personal Data takes the meaning in the UK GDPR which is the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (United Kingdom General Data Protection Regulation), as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (and see section 205(4)).

b) The Parties shall comply with the terms of Part 2 of this Schedule 1 in relation to data security.

5. Invoicing

The Council shall invoice the Client annually in advance for the Services.

6. The Services

a) The Council’s Schools Support Team will:

i. grant to the Client a non-exclusive, non-transferable right, without the right to grant sub licences, to access and use the GovernorHub software for the duration of the Agreement solely for the Client's internal business operations.

b) The Client will:

i. provide the Council's School Support Team with a both a named primary point of contact and finance point of contact.
ii. pay all invoices within 30 days of receipt.
iii. not do anything, or omit to do anything, that would put the Council in breach of its agreement with The Keys Support Service Limited for GovernorHub software and the Client agrees to indemnify the Council in respect of all demands, losses, charges, damages, costs and expenses and other liabilities (including, but not limited to, any professional and/or legal costs and disbursements) the Council incurs as a result of any breach by the Client of this clause 6(b)(iii).

PART 2: 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 (as defined in Part 1 paragraph 4(a) of this Schedule 1).

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 to 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.