ICT AND CYBER SECURITY POLICY

This Policy sets out the Trust's overarching approach to **IT and cyber security**. It establishes the expectations and controls required to protect the Trust's systems, devices, networks and information from cyber threats, unauthorised access, data loss and disruption, and ensures that technology is used securely, responsibly and effectively across all Trust schools and services.

This policy was approved as follows:			
Approver:		**Date: August 2026**	
Owner:	CEO	**Version:**	V1.1
Status:	Non-statutory	**Review frequency:**	Annual
		Next review date:	Sept 2027

This policy applies to all Innovate2Educate Partnership schools, central team employees, Trustees, local governors, workers, volunteers, contractors and pupils when using IT in connection with Trust activity.

Document History

Version	Version Date	Author	Summary of Changes
V1.1	August 2026	CEO	New Policy

1. Purpose

Innovate2Educate Partnership ("i2e") is committed to protecting its digital technology, systems, information and users from cyber security threats, accidental loss, unauthorised access, misuse and disruption.

The purpose of this Policy is to establish the principles and minimum requirements by which i2e manages ICT and cyber security across the Trust and its academies.

The Policy supports the Trust's obligations relating to safeguarding, data protection, financial governance, business continuity, information and records management, and the secure and effective use of digital technology. Detailed technical configurations and incident-recovery procedures may be maintained separately so that they can be updated as technology and risks change.

2. Scope

This Policy applies to all i2e academies and central Trust functions; trustees and governors; employees; temporary and agency staff; volunteers; contractors and consultants; pupils and students where applicable; third parties with authorised access to Trust systems; and organisations providing ICT, cloud or digital services to i2e.

It applies to all Trust digital technology and information, including computers, laptops and tablets; mobile devices; servers and storage; networks and wireless systems; cloud services; email and communication systems; management information systems; finance and HR systems; safeguarding systems; software and applications; removable storage; backups; and other equipment connected to Trust networks or processing Trust information.

3. Policy principles

i2e will take proportionate technical and organisational measures to protect confidentiality, integrity and availability. ICT and cyber security will be managed on a risk-based basis and will have regard to current Department for Education Digital and Technology Standards, National Cyber Security Centre guidance and applicable data-protection and safeguarding requirements.

4. Governance and responsibilities

Board of Trustees: strategic oversight of cyber and digital risk and assurance that appropriate controls, resources and arrangements are in place.

Chief Executive Officer: overall executive responsibility for ensuring appropriate ICT and cyber-security arrangements are established across the Trust.

Senior digital/ICT lead: oversight of digital technology and cyber security across i2e and coordination with senior leaders, the DPO, safeguarding leads and ICT support.

ICT support/provider: implementation and maintenance of appropriate technical controls within the scope of the services provided; responsibilities must be clearly defined where ICT services are outsourced.

Data Protection Officer: advice on data-protection requirements including security of personal data, DPIAs, records of processing activities and personal-data breaches.

Designated Safeguarding Leads: ensuring cyber-security arrangements support safeguarding duties including filtering and monitoring.

All users: compliance with this Policy and Acceptable Use arrangements, protection of credentials and devices, use of authorised systems, prompt reporting of concerns and completion of required training.

5. Cyber risk management

i2e will maintain an appropriate assessment of cyber risk covering its technology, systems, information, users and significant suppliers. A formal cyber-security risk assessment will be undertaken at least annually and additionally following significant technological or organisational change or a significant cyber incident. Cyber risks will be reviewed during the year, including at least termly, to identify material changes, emerging vulnerabilities and actions required. Relevant risks will be recorded within the Trust's risk-management arrangements and escalated to senior leadership or the Board as appropriate.

6. ICT asset and system management

The Trust will maintain appropriate and up-to-date information about its digital technology, including hardware, software, cloud services, critical systems, licences, system owners, suppliers and significant information assets. Unsupported, obsolete or unlicensed hardware and software must not remain in operational use unless expressly authorised following documented risk assessment and appropriate mitigating controls.

7. User accounts and access control

Access to Trust systems and information will be based on legitimate business or educational need and the principle of least privilege. Users will normally be provided with individual accounts. Authentication credentials must not be shared. Shared accounts should be avoided and used only where there is a justified operational requirement and appropriate controls are in place. Access rights must be appropriate to the user's role and reviewed when roles change or access is no longer required. Access for leavers must be removed or disabled promptly. Administrator and other privileged access will be restricted to persons who require it and privileged accounts should not normally be used for routine everyday activity.

8. Passwords and authentication

Users must protect passwords and other authentication credentials from disclosure. Passwords must meet the Trust's approved security requirements, must not be shared, and must be changed promptly where compromise is suspected. Multi-factor authentication (MFA) will be implemented for accounts and services in accordance with current DfE/NCSC cyber-security requirements and the Trust's assessed risks. Users must not attempt to bypass MFA or other authentication controls.

9. Software, security updates and vulnerability management

Only authorised and appropriately licensed software and applications may be installed or used for Trust purposes. ICT support will maintain processes to ensure that operating systems and software remain supported; security updates and vulnerability fixes are applied within appropriate timescales; critical and high-risk vulnerabilities are prioritised; unsupported technology is upgraded, replaced, isolated or otherwise appropriately managed; and users cannot circumvent security controls or install unauthorised software where restrictions are required.

10. Anti-malware, firewalls and network protection

Appropriate protection against malicious software and unauthorised network access will be maintained. Network-connected devices will, where appropriate, be securely configured, use current security protection, be protected by appropriate firewalls, be monitored for malicious or suspicious activity, restrict unnecessary services and access, and prevent users from disabling essential security controls. Email systems will be configured to reduce the risks of phishing, spoofing, malware and other malicious communications.

11. Devices and physical security

Trust devices must be appropriately secured against theft, loss, damage and unauthorised access. Users must lock their screen or device when leaving it unattended, not leave devices containing confidential information unsecured, take reasonable care when transporting Trust equipment, report loss or theft immediately, comply with Trust arrangements concerning use outside Trust premises, and not allow unauthorised persons to use Trust equipment or accounts. Appropriate encryption must be used where required.

12. Approved systems and cloud services

Trust information must be created, processed and stored only within approved systems and services. Staff must not introduce or use new cloud services, applications, generative AI services or other digital products to process Trust personal, confidential or safeguarding information without appropriate approval. New systems processing personal data must be considered within the Trust's data-protection arrangements, including lawful processing, information security, supplier arrangements, records of processing activities, data retention, international transfers where applicable, and a Data Protection Impact Assessment where required.

13. Removable media

Removable storage media, including USB drives, should only be used where there is a genuine operational need and an approved secure alternative is not reasonably available. Where removable media is authorised, only Trust-approved devices may be used, appropriate encryption must be applied, sensitive data must be protected, the device must be stored securely, information must be securely deleted when no longer required, and loss or theft must be reported immediately.

14. Personal devices

Personal devices may only be used for Trust business where permitted by the Trust's approved arrangements. Where authorised, appropriate security controls must be applied and users must comply with data-protection, safeguarding and acceptable-use requirements. Trust personal, safeguarding or confidential information must not be stored locally on personal devices unless expressly authorised and appropriately protected.

15. Email and secure communications

Users must exercise particular care when sending personal, safeguarding, financial or confidential information electronically. Before sending information, users must check the identity and address of the recipient, ensure the recipient is entitled to receive the information, use an approved secure method where appropriate, avoid unnecessary disclosure, and follow Trust procedures for secure data sharing. Suspicious emails, links, attachments, requests for credentials or unusual payment instructions must be treated with caution and reported promptly.

16. Backups and recovery

i2e will maintain backup arrangements appropriate to its systems, information and operational requirements. The Trust will have a documented backup approach identifying the systems and information requiring backup, appropriate backup frequency, retention arrangements, responsibilities, protection of backups from unauthorised access, alteration or deletion, arrangements designed to reduce the risk of ransomware affecting both live and backup data, and recovery requirements. Backup arrangements must include appropriate testing to demonstrate that information and systems can be restored and must be reviewed at least annually and following significant changes to systems or risks.

17. Digital continuity and system change

When systems, applications or storage arrangements are replaced or decommissioned, i2e will ensure that information which remains subject to a legal, regulatory, safeguarding, business or retention requirement continues to be accessible, readable, secure, complete and usable. Appropriate migration, export or preservation arrangements must be considered before systems containing important Trust records are withdrawn. Digital continuity will be managed alongside the Trust's Records Management & Retention Statement.

18. Filtering and monitoring

i2e will maintain appropriate filtering and monitoring arrangements in accordance with current safeguarding legislation and statutory guidance, Keeping Children Safe in Education, current Department for Education Filtering and Monitoring Standards, and the Trust's Online Safety and Safeguarding arrangements. Responsibilities for filtering and monitoring will be clearly assigned and provision will be reviewed at least annually and following material changes or concerns.

19. Suppliers and third-party access

Cyber-security and data-protection risks must be considered when appointing ICT, cloud and other digital service providers. Appropriate contractual and security arrangements will be established where suppliers access Trust systems, process Trust information, host information or provide critical services. Third-party access must be limited to what is necessary and removed when no longer required.

20. Cyber-security incidents

All actual or suspected cyber-security incidents must be reported immediately through the Trust's established reporting arrangements. Staff should report concerns promptly rather than attempting to investigate or remedy significant incidents themselves.

21. Cyber Security Recovery Plan

Significant cyber-security incidents will be managed in accordance with the Trust's Cyber Security Recovery Plan and, where appropriate, its wider business-continuity arrangements. The Recovery Plan will establish operational arrangements for incident escalation, containment, preservation of evidence, communication, system recovery, restoration of data, involvement of external ICT or specialist support, regulatory and other reporting, and lessons learned following an incident. The Recovery Plan will be maintained as a separate operational document and reviewed and tested regularly.

22. Personal data breaches

Where a cyber-security incident involves, or may involve, personal data, the Data Protection Officer or appropriate data-protection lead must be informed without delay. The incident will be assessed under the Trust's Personal Data Breach procedures. Where legally required, the Information Commissioner's Office will be notified within the applicable statutory timescale and affected individuals will be informed where required.

23. Fraud, cybercrime and ransom demands

The Trust will maintain proportionate controls to manage the risk of cybercrime and will take appropriate action where cybercrime is suspected or identified. Relevant incidents will be reported to the appropriate authorities, insurers, Risk Protection Arrangement and Department for Education where applicable. i2e will not pay ransom or extortion demands, including ransomware demands.

24. Training and awareness

All relevant staff will receive appropriate and regularly updated cyber-security and data-protection awareness training. Training will cover, as appropriate, phishing and social engineering; password and MFA security; protection of devices; safe use of email and digital communications; removable media; reporting cyber incidents; reporting personal-data breaches; secure handling of information; and current and emerging cyber risks. Additional training will be provided to staff with privileged access or higher-risk responsibilities.

25. Acceptable use

All users must comply with the Trust's Acceptable Use arrangements. Users must not attempt to bypass security, filtering or monitoring controls; access systems or information without authority; install unauthorised software; deliberately introduce malicious software; share authentication credentials; use Trust systems for unlawful activity; or take actions which knowingly expose the Trust to unreasonable cybersecurity risk.

26. Monitoring, assurance and audit

Compliance with this Policy and the effectiveness of the Trust's cyber-security arrangements will be monitored through appropriate assurance processes. These may include cyber-risk assessments, technical security reviews, vulnerability assessments, review of access rights, backup and recovery testing, incident analysis, audit, supplier assurance, monitoring against DfE Digital and Technology Standards, and reporting to senior leadership and Trustees.

27. Review of this Policy

This Policy will be reviewed at least annually for continued technical and regulatory relevance and formally reviewed in accordance with the Trust's policy-review arrangements. An earlier review will be undertaken where required following a significant cyber-security incident, significant change to technology or infrastructure, material changes to DfE, NCSC or ICO requirements, changes to applicable legislation, significant audit findings, or material changes to the Trust's operating arrangements.

28. Related Trust documents

This Policy should be read alongside, as applicable:

- Cyber Security Recovery Plan
- Records Management & Retention Statement
- Data Protection Policy
- Personal Data Breach Procedure
- Online Safety Policy
- Safeguarding and Child Protection Policy
- Acceptable Use arrangements
- Business Continuity Plan
- Freedom of Information Policy
- Staff Code of Conduct
- relevant procurement and supplier-management arrangements

29. Legislative and regulatory framework

i2e will have regard to current applicable legislation, statutory guidance and national standards, including:

- UK General Data Protection Regulation
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- applicable safeguarding legislation
- current Keeping Children Safe in Education statutory guidance
- current Academy Trust Handbook
- Department for Education Digital and Technology Standards
- Department for Education Cyber Security Core Standard

- Department for Education Filtering and Monitoring Core Standard
- Department for Education Data Protection in Schools guidance
- National Cyber Security Centre guidance
- Information Commissioner's Office guidance
- applicable Risk Protection Arrangement requirements

Where legislation, statutory guidance or mandatory requirements are amended or replaced, the current requirements will apply.