CYBER SECURITY POLICY

ORGINATOR: GARY STONE
SLT LINK: STUART WILLIAMS

June 2026

RUTLAND AND DISTRICT SCHOOLS' FEDERATION

CONTENTS

1. PURPOSE

Rutland & District Schools' Federation recognises that cyber security is essential to the safe and effective operation of teaching, learning and administrative functions within its schools. The purpose of this policy is to set out the Federation's approach to protecting its information systems and services from cyber threats including phishing, malware, ransomware, unauthorised access, data loss, service disruption, and other digital security incidents.

This policy is intended to ensure that the Federation maintains the confidentiality, integrity and availability of its information and digital systems. It also supports compliance with the Department for Education's cyber security standards for schools and colleges, aligns with National Cyber Security Centre principles, and reflects common baseline controls found in Cyber Essentials.

The Federation acknowledges that cyber incidents can lead to safeguarding concerns, reputational damage, financial loss, operational disruption, and legal or regulatory breaches. For that reason, cyber security is treated as both a priority across the organisation.

2. SCOPE

This policy applies to all members of the Federation community, including:

- Employees
- Agency staff
- Governors
- Volunteers
- Contractors
- Pupils
- Or any third parties who are granted access to Federation systems.

It covers all Federation-owned and Federation-managed digital resources, including but not limited to

- Servers
- Desktop & laptop computers
- Mobile devices, including tablets
- Network infrastructure
- Cloud services, email systems
- Safeguarding and student management systems
- Telephones, internet services
- Backup systems
- Any personal devices that are authorised to connect to Federation systems.

This policy also applies to cyber security risks arising from remote working, home use of school systems, supplier access, cloud-hosted services, and the transmission or storage of Federation information outside the physical school site.

3. ROLES AND RESPONSIBILITIES

3.1 Trustees

Trustees retain overall responsibility for ensuring that appropriate cyber security arrangements are in place. This includes approving the policy, receiving assurance that risks are being managed, ensuring sufficient resources are allocated, and confirming that cyber risk is considered as part of wider corporate governance and risk oversight.

3.2 Executive Principal and the Senior Leadership Team

The Executive Principal and the Senior Leadership Team are responsible for embedding this policy in practice, ensuring cyber security remains a leadership priority, and supporting a culture in which staff understand their responsibilities. SLT will review risks, receive incident reports, and ensure that policy, staffing, procurement and operational decisions take cyber security into account.

3.3 Technologies Director

The Technologies Director is responsible for coordinating the Federation's cyber security arrangements. This includes maintaining the cyber risk register, advising leaders on emerging threats, overseeing security controls, coordinating incident response, ensuring

appropriate staff awareness activity, and acting as a point of contact with external support providers where required.

3.4 IT Support team

The IT Support team is responsible for the technical implementation of security controls, including secure configuration, patch management, anti-malware, account administration, backup operations, monitoring, and remediation of vulnerabilities. The IT function will also support investigations into cyber incidents and ensure appropriate controls remain operational.

3.5 Other stakeholders

All staff, governors, pupils and other users are responsible for complying with this policy, using technology safely and responsibly, protecting passwords and devices, reporting suspicious activity promptly, and completing any training required by the Federation. Cyber security is not solely a technical issue; it is a shared responsibility across the whole organisation.

3.6 Data Protection

The Federation will protect personal and sensitive data in accordance with UK GDPR, the Data Protection Act 2018, and internal information governance requirements. Information will only be accessed, processed, stored, transferred and retained where there is a lawful and legitimate reason to do so, and only by those with appropriate authorisation.

The Federation recognises that cyber security and data protection are closely linked. Weak cyber controls can result in personal data breaches, safeguarding concerns, service interruption. For that reason, sensitive data will be subject to proportionate measures such as access restriction, encryption, secure sharing arrangements, retention controls and disposal procedures.

Particular care will be taken with safeguarding records, SEN information, staff HR data, medical information, financial records and any data that if exposed, could cause harm to individuals or to the Federation. Staff must comply with any related data protection, confidentiality and records management policies. Details of which can be found in the Federation ICT Code of Conduct and Data Protection Policy.

3.7 Cyber Risk Management

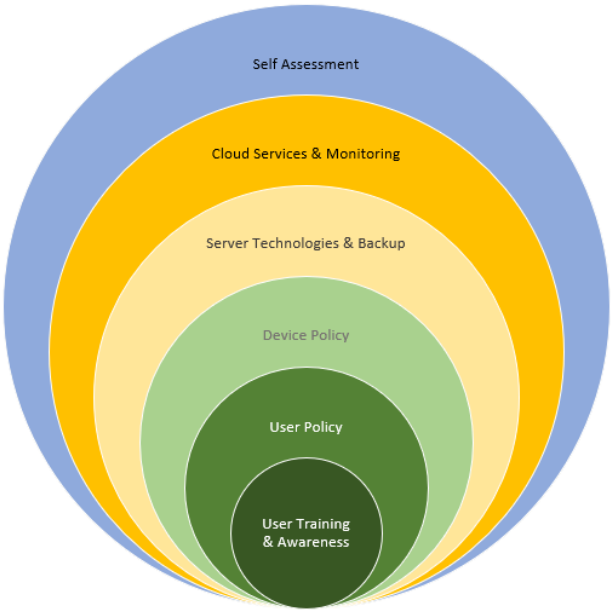
The Federation will manage cyber security through a formal, risk-based approach. Cyber risks will be identified, assessed, recorded and reviewed in the same way as other strategic risks to the organisation in the federation Live Risk Register. A cyber incident is capable of affecting safeguarding, finance, operations, teaching continuity and legal compliance, and must therefore be reflected within the Federation's wider organisational risk management strategy.

A formal cyber risk assessment will be carried out at least annually, with interim sooner where there is a substantial change to systems, staffing or threat intelligence. Risks will

be recorded in the organisational risk register with a named owner. Incidents will be reported to the Executive Principal and trustees.

The Federation will consider risks arising from human behaviour, technical vulnerabilities, remote access, unsupported systems, weak access control, inadequate backups, supplier dependency, data handling, cloud systems, and online safety/safeguarding implications. Cyber risks will be reported to leaders and trustees in an appropriate format to support decision-making and resource allocation.

The Federation will take a layered approach to constantly improve cyber resilience.



4. TECHNICAL SECURITY CONTROLS

The Federation will maintain an appropriate set of baseline technical controls to reduce the likelihood and impact of cyber incidents. These controls will include, as a minimum:

- Secure network boundary
- Anti-malware/anti-virus
- Patch management
- Secure configuration
- Access controls
- System monitoring
- Modern device security
- Data backup

4.1 Secure Network Boundary

The Federation network will be protected by suitably configured firewalls and secure wireless technologies, all default passwords will be changed. Network design will seek to reduce unnecessary exposure between systems and users. Where appropriate,

segmentation and access rules will be used to reduce lateral movement when a system is compromised.

4.2 Endpoint Security

All Federation-managed devices will be configured in line with security best practice and protected by up-to-date anti-malware or equivalent endpoint security tools, including Software based firewalls blocking external access to all endpoints. Devices must not be used in a way that introduces unauthorised software, weakens security settings or bypasses Federation safeguards. This is outlined further in the Federation ICT Code of Conduct

4.3 Patch Management

Operating systems, applications, browsers, firmware and network devices will be kept up to date. Security patches will be applied in line with risk and severity, with critical vulnerabilities prioritised. Unsupported or end-of-life software and hardware will be removed, replaced or risk-managed using additional control measures.

4.4 Secure Configuration

Systems and services will be securely configured before deployment and reviewed regularly thereafter. Default settings, unnecessary software, unused user accounts, open services and excessive privileges will be minimised wherever possible. Cloud platforms such as Microsoft 365 will be configured with security controls appropriate to the sensitivity of the data and the role of the service.

4.5 Access Control

Each user will be allocated a unique account and access rights appropriate to their role. Additional privileged accounts will be given where escalated, system access if required. Access will be tightly controlled, kept to the minimum necessary, and reviewed on a regular basis. Strong passwords and multi-factor authentication will be used for staff accounts, remote access and higher-risk systems. Accounts for leavers will be disabled promptly at the end of their last contracted day.

4.5 Monitoring and Detection

The Federation will monitor network, system and account activity to support the detection of suspicious behaviour, safeguarding concerns, technical faults, misuse, attempted compromise and other cyber-related issues. Monitoring may include logs from endpoints, firewalls, cloud services, email systems, filtering systems, and identity platforms.

Monitoring arrangements will be proportionate, lawful and aligned to school responsibilities, including the Department for Education expectations relating to filtering and monitoring. Where alerts or anomalies are detected, they will be reviewed and escalated according to risk. Log retention and access arrangements will support investigation and accountability.

The Federation will ensure that monitoring information is accessible only to authorised personnel and is used for legitimate safeguarding, compliance and security purposes.

4.6 Modern Device Security

All Federation devices will be managed using modern security controls to ensure they remain secure, compliant and resilient against emerging threats. Devices must be enrolled in centrally managed endpoint or mobile device management systems to enforce security policies including encryption, patching and application control. Access to Federation systems may be restricted based on device compliance, ensuring that only devices meeting defined security standards are permitted to connect.

4.7 Backup and Disaster Recovery

The Federation will maintain reliable and proportionate backup arrangements for critical data and systems. Backups will be configured to support recovery from incidents including ransomware, accidental deletion, corruption, hardware failure and other service-impacting events. Backup arrangements will be appropriate to the operational importance of the data or service.

Critical data will be backed up regularly and stored securely, with at least one form of backup protected from routine online compromise on offline and/or immutable storage. Backup success will be monitored and tested on a regular basis and logged in the IT Assets Register.

The Federation have defined recovery priorities so that safeguarding, communication and key operational systems can be restored in a planned order. Backup and recovery arrangements will form part of the Federation's wider resilience and continuity planning. These are outlined in the Federation Cyber Recovery Plan.

5. INCIDENT RESPONSE

The Federation will maintain a clear and structured approach to cyber incident response in order to reduce harm, restore normal service quickly and learn from events. A cyber incident may include, but is not limited to:

- Phishing compromise
- Malware infection
- Ransomware
- Data breach
- Account compromise
- Denial of service
- Loss or theft of a device
- Unauthorised access
- Suspicious monitoring alerts or any event giving rise to concern about the confidentiality, integrity or availability of data or systems.

The Federation will manage incidents through a staged process:

- Identify
- Contain
- Eradicate
- Recover
- Review

Staff must report any suspected cyber incident immediately to the Technologies Director or designated IT contact. Prompt reporting is essential to limit spread, preserve evidence, maintain safeguarding continuity and reduce recovery time.

5.1 Identify

The Federation will maintain mechanisms to identify cyber concerns through staff reports, technical monitoring, alerts from suppliers, unusual device or account behaviour, and evidence of data compromise or service disruption. Staff will be trained to recognise signs of phishing, suspicious links, abnormal login activity, data loss or other warning indicators.

5.2 Contain

Where an incident is suspected, the Federation will act quickly to contain the risk. This may include isolating devices, disabling accounts, blocking malicious domains, suspending access, withdrawing remote sessions, or disconnecting systems from the network where necessary. Containment decisions will balance operational need with the need to protect users, data and evidence.

5.3 Eradicate

The Federation will remove the cause of the incident wherever practicable. This may involve malware removal, patching, password resets, rebuilding systems, correcting configuration weaknesses, removing unauthorised applications or working with suppliers and specialist support where appropriate.

5.4 Recover

The Federation will restore affected services in a controlled way, using backups and recovery procedures where required. Recovery will prioritise systems essential to safeguarding, communication, finance and core school operations. The Federation will verify that restored systems are secure and functioning before returning them fully to live use.

5.5 Review

Every significant incident will be reviewed to identify root causes, lessons learned and recommended improvements. Outcomes will inform risk assessment, training, technical changes, procurement decisions and future assurance activity.

5.6 Reporting

Incidents will be recorded and escalated in accordance with severity. External reporting will be made where required including to the DfE, the NCSC and/or the Information Commissioner's Office in the event of relevant personal data breaches or serious incidents.

6. ASSET MANAGEMENT

The Federation will maintain an up-to-date record of key information assets and technology assets, including devices, platforms, services, major applications, and systems storing or processing sensitive data. Asset management supports security by ensuring the Federation understands what it owns, what it uses, who is responsible for it and which systems require protection, upgrade or replacement.

The Federation will minimise the use of unsupported systems and ensure that devices leaving service are securely wiped, returned, recycled or disposed of in accordance with data protection and environmental requirements.

7. STAFF TRAINING AND AWARENESS

The Federation recognises that most cyber incidents in education have a significant human factor. Staff awareness is therefore a key security control. All staff will undertake regular cyber security awareness training, including induction training for new starters and periodic refreshers thereafter.

Training will cover areas such as phishing, password security, safe use of devices, data handling, incident reporting, remote working, secure sharing, and the risk of social engineering. The Federation may supplement training with briefings, alerts, awareness campaigns or simulated phishing exercises where appropriate.

Pupils will receive age-appropriate online safety and cyber awareness education through the curriculum and associated safeguarding work. Leaders will ensure that relevant staff, including safeguarding staff and those handling sensitive data, receive a level of awareness proportionate to their role.

8. SUPPLIER AND THIRD-PARTY SECURITY

The Federation relies on a range of suppliers, cloud providers and service partners to deliver technology and business services. These relationships can introduce cyber and data protection risks if not properly governed. The Federation will therefore apply reasonable due diligence to suppliers who store, process, access or support Federation data or systems.

Contracts and service arrangements should, where appropriate, include expectations relating to confidentiality, data handling, access control, support arrangements, breach notification, and compliance with applicable UK data protection requirements. Supplier access to Federation systems will be limited to what is necessary and reviewed regularly.

The Federation will seek assurance, where proportionate, that significant technology suppliers have appropriate security arrangements in place, especially where services support safeguarding, identity, communication, finance, cloud productivity, or storage of sensitive data.

9. BUSINESS CONTINUITY

The Federation acknowledges that a serious cyber incident could disrupt teaching, safeguarding, communication, finance and trust operations for an extended period. Cyber resilience therefore forms part of the Federation's wider business continuity planning. Recovery arrangements will take account of the need to maintain safe operation, communication with stakeholders, and continuity of essential services.

Continuity planning will identify critical systems, minimum operational requirements, fallback arrangements, communication methods and recovery priorities. Particular attention will be given to safeguarding systems, management information systems, payroll and finance systems, communication channels, and tools that support teaching and learning.

Where systems are unavailable, the Federation will use alternative procedures where practicable until normal service is restored. The Federation will review continuity lessons following incidents or exercises and update plans accordingly.

10. COMPLIANCE AND REVIEW

This policy should be read alongside related Federation policies and procedures, including those covering:

- Data Protection
- Federation ICT Code of Conduct
- Financial Management
- Safeguarding
- Records Retention
- Business Continuity Planning

Cyber security depends on the combined operation of these controls rather than on a single document in isolation.

The Federation will keep this policy under regular review to ensure it reflects current risk, legal obligations, DfE standards, operational practice and the changing technology landscape. It will be reviewed at least annually, and additionally following major incidents, significant changes in systems or suppliers, or relevant changes in legislation or national guidance.

The Federation will seek continuous improvement through policy review, audit, risk assessment, incident review, training evaluation and benchmarking against recognised frameworks and good practice, including DfE standards and Cyber Essentials-style controls.