Cyber Security Policy

Stanton Bridge Primary School

Policy owner	Emma Good, Assistant Headteacher
Approved by	
Updated	April 2026
Next review	April 2027

This policy should be read alongside the School's Data Protection, Data Breach, Information Security, Acceptable Use and Business Continuity policies.

Document Control

Version	Date	Summary of changes
1.0	April 2026	New policy issued and strengthened to reflect current cyber-security expectations.

Document Ownership and Approval

Emma Good, Assistant Headteacher, is the owner of this document and is responsible for ensuring that it is reviewed in accordance with the School's policy review schedule.

The current version of this policy is available to all members of staff at the following location:

Stanton_Bridge_Cyber_Security_Policy_April_2026_Updated.docx

Printed copies may become out of date. Staff should refer to the centrally stored electronic version wherever possible.

Contents

1. Cyber Security Policy

Cyber security has been identified as a significant risk to the School. Every employee, trustee and authorised user has a responsibility to contribute to the security of the School's data, systems and equipment.

The School has invested in technical cyber-security measures. However, technical controls alone cannot provide complete protection. All users must remain vigilant and take appropriate steps to protect the School's information technology systems.

The Assistant Headteacher with responsibility for cyber security will coordinate the School's approach, supported by the Headteacher, Data Protection Officer, IT support provider and other relevant staff, as appropriate.

Employees may be subject to disciplinary action if they breach this policy.

This policy should be read alongside the School's:

- Data Protection Policy;
- Data Breach Policy;
- Information Security Policy;
- Acceptable Use Policy;
- Information and Communications Policy;
- Business Continuity Plan; and
- relevant safeguarding and filtering and monitoring procedures.

Cyberbullying involving pupils will be treated as seriously as any other form of bullying and will be managed through the School's anti-bullying procedures, as outlined in the Behaviour Policy.

2. Purpose and Scope

The purpose of this policy is to establish systems and controls to protect the School from cybercriminals and associated cyber-security risks. It also sets out the action that will be taken if the School experiences a cyber-security incident.

This policy applies to all staff, trustees, volunteers, contractors, visitors and other authorised users of the School's systems.

3. What Is Cybercrime?

Cybercrime is criminal activity carried out using computers, digital devices, networks or the internet. It may include:

- hacking;
- phishing;
- malware;
- computer viruses;
- ransomware;
- unauthorised access;
- data theft;
- identity theft;
- denial-of-service attacks; and
- other attempts to disrupt, damage or misuse systems or information.

Cybercrime and cyber-security incidents may result in the following consequences.

3.1 Financial cost

Cyber incidents may result in financial loss, including recovery costs, loss of income, fraud, legal claims, contractual penalties or regulatory fines.

Serious breaches of data-protection legislation may result in significant regulatory action. The maximum fine available under the UK GDPR may be £17.5 million or, in the case of an undertaking, 4% of its total worldwide annual turnover, whichever is higher.

3.2 Confidentiality and data protection

Protecting confidential information and personal data is one of the School's most important responsibilities. A cyber incident could result in information being lost, altered, disclosed, encrypted or accessed without authorisation.

3.3 Regulatory breaches

The School has a range of legal and regulatory responsibilities. A cyberattack or other security incident could cause the School to breach these responsibilities.

The loss or unauthorised disclosure of personal data may also result in complaints, claims for compensation, regulatory investigation or enforcement action by the Information Commissioner's Office.

3.4 Reputational damage

A cyber-security incident can have a significant impact on the School's reputation, particularly if it involves confidential information or personal data, or is reported publicly or in the media. Protecting the School's reputation and maintaining the confidence of pupils, families, staff and the wider community are of utmost importance.

3.5 Business interruption

Some forms of cyberattack may make key systems unavailable. These may include:

- servers;
- email systems;
- cloud-based services;
- management information systems;
- safeguarding systems;
- telephone systems;
- teaching and learning platforms; and
- the School's website.

A significant disruption could affect the delivery of lessons, safeguarding arrangements, communications and other essential School services.

Where appropriate, the Headteacher will decide whether to invoke the School's Business Continuity Plan, in consultation with relevant senior leaders and the IT support provider.

3.6 Organisational and financial instability

Financial losses and prolonged disruption resulting from cybercrime may place considerable pressure on the School's staffing, operations, finances and resources.

4. Cybercrime Prevention

Given the seriousness of these potential consequences, the School will take appropriate preventative measures. All users must follow the expectations and guidance contained within this policy.

The School will work towards meeting the Department for Education's digital and technology standards, including the cyber-security core standard.

The School has implemented technical measures, organisational controls and staff guidance to reduce the likelihood and potential impact of cybercrime.

5. Technical Security Measures

Subject to the School's systems, contracts and arrangements with its IT support provider, security measures will include:

1. firewalls;
2. antivirus and anti-malware software;
3. anti-spam and email-security software;
4. automatic or timely security updates for systems and applications;
5. web-filtering and monitoring systems;
6. regular, secure and tested data backups;
7. encryption, where appropriate;
8. the prompt deletion or disabling of unused user accounts;
9. the removal or disabling of unnecessary or unsupported software;
10. strong and unique passwords;
11. multi-factor authentication;
12. disabling unnecessary auto-run features;
13. appropriate access controls and user permissions;
14. logging and monitoring of system activity, where appropriate;
15. secure configuration of devices and networks; and
16. procedures for securely disposing of equipment and data.

Backups will be protected from unauthorised access and, where appropriate, separated from the live network. Restoration procedures will be tested periodically to ensure that data can be recovered following an incident.

6. Controls and Guidance for Staff

Technical solutions alone cannot adequately protect the School. Systems and controls must also address the human element of cyber-security risk.

All staff will receive appropriate cyber-security training:

- as part of their induction;
- through periodic refresher training;
- following significant changes to legislation, guidance or School policy;
- when significant new threats are identified; and
- following an incident affecting the School or an organisation with which the School shares information.

Access to systems and information will be limited according to the user's role and responsibilities.

Where particularly sensitive information is involved, the School may introduce additional controls. These may include:

- limiting the number of people who have access to the information;
- separating particular work areas or teams where appropriate;
- ensuring that systems for receiving, opening, distributing and scanning correspondence do not result in the inadvertent disclosure of confidential information;
- requiring confidentiality agreements where appropriate;
- securely disposing of confidential documents;
- operating a clear-desk and clear-screen approach;
- ensuring that confidential papers are not read in public places;
- ensuring that sensitive matters are not discussed where they may be overheard; and
- conducting appropriate due diligence on organisations with which the School shares information.

7. Staff Responsibilities

All staff must:

- report cyber-security concerns or incidents promptly using the School's agreed reporting procedure;
- understand the risks presented by cybercrime and cyber-security incidents;
- take reasonable and proportionate action to reduce those risks;
- complete all required cyber-security training;
- comply with the School's password requirements;
- use strong, unique passwords or passphrases;
- keep passwords and authentication codes confidential;
- not reuse School passwords for personal accounts;
- never allow another person to access School systems using their login details;
- use multi-factor authentication where it is available or required;
- lock their computer or device when leaving it unattended;
- verify unexpected requests for payments, password changes or confidential information through a separate and trusted method of communication;
- exercise caution before opening attachments, scanning QR codes or clicking links;
- report suspicious emails, messages, telephone calls or login requests;
- not disable, alter or attempt to circumvent security controls installed by the School or its IT support provider;
- immediately report any suspected breach, suspicious activity, lost device or mistake that may result in a cyber-security or data-protection incident;
- follow the Data Breach Policy where an incident involves or may involve personal data;
- only use authorised devices and systems to access School information;
- only connect personal devices to wireless networks specifically authorised for personal or visitor use;
- not install software, applications, browser extensions or other programs on School equipment without authorisation;
- not connect unauthorised storage devices or equipment to the School's systems;
- avoid accessing inappropriate content or downloading unauthorised or unusually large files using School equipment or networks;
- store School information only in approved locations;
- not use personal email accounts or unauthorised cloud-storage services for School information; and
- follow any instructions issued by senior leaders or the IT support provider during a cyber-security incident.

Concerns must be reported as soon as possible to Emma Good or, in her absence, to the Headteacher, Data Protection Officer or another designated senior leader.

8. Misuse of School Systems

The School considers the following to be misuse of its IT systems or resources:

- carrying out malicious, unlawful or unauthorised activity against the School or using School systems;
- accessing, creating, storing or distributing inappropriate, adult or illegal content on School premises or using School equipment;
- excessive or inappropriate personal use of School systems during working hours;
- removing data or equipment from School premises or systems without permission;
- using School equipment in a manner prohibited by this or another School policy;
- attempting to bypass filtering, monitoring, access controls or other cyber-security measures;
- sharing passwords or authentication information;
- accessing information without a legitimate work-related reason;
- installing unauthorised software or hardware;
- failing to follow reasonable security instructions; and
- deliberately or negligently failing to report a suspected incident or security breach.

Misuse may result in access being suspended or withdrawn and may lead to disciplinary action. Where appropriate, the matter may also be reported to the police, regulators or other relevant organisations.

9. Cyber-Security Incident Management Plan

All suspected cyber-security incidents must be reported immediately. Staff should not attempt to investigate an incident themselves unless instructed to do so.

Where appropriate, the School's response will consist of the following stages.

9.1 Identification, containment and recovery

This may include:

- establishing what has happened;
- disconnecting affected equipment from the network where advised;
- preventing further unauthorised access;
- preserving relevant evidence and system logs;
- obtaining assistance from the IT support provider or specialist advisers;
- recovering systems and data from secure backups;
- notifying insurers as soon as reasonably practicable where the incident may give rise to a claim; and
- considering whether to invoke the Business Continuity Plan.

Devices must not be wiped, reset or altered unless this has been authorised by the IT support provider or incident lead.

9.2 Assessment of risk

The School will assess:

- the nature and cause of the incident;
- the systems, accounts and information affected;
- whether personal or confidential data has been affected;
- whether affected data was encrypted or otherwise protected;
- the number and categories of individuals affected;
- the likely consequences for individuals and the School;

- whether the incident is continuing; and
- what immediate and longer-term action is required.

9.3 Notification and communication

The School will consider whether the incident must or should be reported to:

- the Information Commissioner's Office;
- affected individuals;
- the Department for Education;
- the National Cyber Security Centre;
- Action Fraud or the police;
- the Local Authority or Trust;
- insurers;
- safeguarding partners;
- parents and carers;
- staff;
- service providers; and
- any other relevant organisation.

Where a personal-data breach meets the threshold for notification, it must be reported to the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of the School becoming aware of it.

All personal-data breaches will be documented, including those that are assessed as not requiring notification to the Information Commissioner's Office.

External communications and media enquiries will be coordinated by the Headteacher or another authorised senior leader.

9.4 Evaluation and improvement

Following an incident, the School will:

- evaluate the effectiveness of its response;
- identify the cause of the incident;
- consider whether any policies, systems or working practices need to change;
- implement appropriate improvements;
- provide further training where required;
- review the effectiveness of suppliers and support arrangements; and
- record lessons learned.

The incident response arrangements will also be reviewed and tested periodically, including where there has not been a recent incident.

10. Personal-Data Breaches

Where a cyber-security incident involves, or may involve, a personal-data breach, the School's Data Breach Policy will be followed alongside this policy.

Following the Data Breach Policy does not prevent the School from taking the immediate technical and operational actions required to contain the cyber-security incident.

11. Monitoring and Review

Compliance with this policy will be monitored by the Assistant Headteacher with responsibility for cyber security, supported by the Headteacher, Data Protection Officer and IT support provider.

The policy will be reviewed:

- annually;
- following a significant cyber-security incident;
- following relevant changes to legislation or statutory guidance;
- following major changes to the School's systems or suppliers; or
- where monitoring identifies that changes are required.

Appendix 1: Immediate Actions for Staff

If you suspect a cyber-security incident:

17. Stop and do not continue entering information.
18. Disconnect the device from the network only if instructed, or if it is safe and clearly necessary to prevent an active attack.
19. Do not switch off, wipe or reset the device.
20. Record what happened, including the time, system and any messages displayed.
21. Report the incident immediately to Emma Good, the Headteacher, the Data Protection Officer or the IT support provider.
22. Follow any instructions provided and preserve relevant emails, screenshots or other evidence.

Appendix 2: Password and Account Security Guidance

All staff and authorised users are responsible for protecting their School accounts.

Creating a secure password

Passwords should:

- be unique to the School account for which they are created;
- be sufficiently long and difficult for another person to guess;
- consist of three or more random, unrelated words where the system permits;
- not contain easily identifiable personal information, such as names, dates of birth, addresses, family members or pets;
- not contain the name of the School, the user's job role or other information closely connected to the user; and
- not rely on predictable substitutions, such as replacing the letter "o" with the number "0".

Staff must comply with any additional password requirements applied by the School's IT systems or IT support provider.

Protecting passwords

Staff must:

- never share a password with another person, including colleagues, managers or IT support staff;
- never disclose passwords or authentication codes by email, telephone, text message or online form;
- not reuse a School password for a personal or external account;
- not allow browsers or applications to save passwords unless this has been authorised by the School;
- use only a School-approved password manager where one has been provided or authorised;
- change a password immediately if there is reason to believe it has been compromised; and
- report any suspected compromise to the designated cyber-security lead or IT support provider immediately.

Multi-factor authentication

Multi-factor authentication or two-step verification must be used wherever it is available or required.

Staff must:

- never approve an unexpected authentication request;
- never disclose a verification code to another person;
- check carefully that a login request relates to an action they have initiated; and
- report repeated or unexpected authentication prompts immediately.

An unexpected authentication request may indicate that another person has obtained, or is attempting to use, the member of staff's password.

Further guidance

Further guidance is available from the National Cyber Security Centre – Three random words webpage.

This appendix should be read alongside the School's Cyber Security Policy, Acceptable Use Policy and Information Security Policy.

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this policy. If you have any questions about how we handle your personal information which cannot be resolved by Emma Good, then you can contact the DPO on the details below:

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk