

Cyber Security Policy



Approved by: Finance and Resources Committee

Last reviewed on: March 2026

Next review due by: March 2027

Date: February 2026

Written by:
John Woolman,
Assistant Headteacher

1. Introduction

A cybersecurity incident can have a significant impact on any organisation for an extended period of time. For a school, this can range from reputational damage and the cost of restoring systems from existing backups, to major incidents such as loss of student work, disruption to learning platforms, or restricted access to safeguarding systems. Such incidents may result in data protection breaches, regulatory consequences or inspection concerns.

This Cybersecurity Policy outlines Elsley Primary School's guidelines and security provisions designed to protect our systems, services and data from cyber threats and to ensure effective response in the event of a cyber incident. Cybersecurity arrangements support the school's safeguarding obligations by ensuring access to safeguarding systems remains protected and resilient.

2. Legislation and Standards

This policy is informed by:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Department for Education (DfE) Filtering and Monitoring Standards (2023)
- National Cyber Security Centre (NCSC) Cyber Security Guidance for Schools
- Keeping Children Safe in Education (KCSIE 2025)

3. Scope of Policy

This policy applies to all Elsley Primary School staff, governors, contractors, volunteers and any other individuals granted permanent or temporary access to school systems, devices or data.

It covers both the physical and technical elements used to deliver IT services across the school.

4. Roles and Responsibilities

The Online Safety Lead is Matt Fortune.

IT Support is provided by Partnership Education Ltd.

The Headteacher retains overall accountability for cyber security, supported by the Online Safety Lead, Leadership Team, the external IT support provider and the Data Protection Officer (DPO).

All users are responsible for the security of their own accounts and devices.

If at any time users believe their credentials may have been compromised (for example following a phishing attempt), they must:

- Change their password immediately; and
- Inform the Headteacher, a member of the Leadership Team, or the Online Safety Lead without delay.

Any suspected cyber incident must be reported immediately to the Data Protection Officer. Where personal data may have been compromised, the DPO will determine whether notification to the Information Commissioner's Office (ICO) is required within statutory timeframes.

Personal accounts must not be used for work-related purposes.

Elsley Primary School will implement multi-factor authentication (MFA) where practicable and appropriate.

5. Risk Management

Elsley Primary School will regularly review cybersecurity risks and ensure these are reflected within the school's risk management processes.

Cyber-related risks and mitigation strategies will be reported to Governors at least annually, or more frequently where significant risk is identified.

6. Physical Security

Elsley Primary School will ensure appropriate physical security and environmental controls are in place to protect access to IT systems. This includes, but is not limited to:

- Secure server and communications rooms
- Locked rooms when the school is closed
- Appropriate environmental protections e.g. ventilation and temperature control (air-conditioning), where required.

7. Asset Management

To ensure that controls are applied effectively, the school will maintain asset registers for:

- Files and systems holding confidential data
- All physical devices (eg servers, switches, PCs, laptops and other network infrastructure)

These registers will support monitoring, maintenance and risk management.

8. Devices

To ensure the security of all school-issued devices and data, users are required to:

- Lock devices when left unattended
- Install updates when prompted
- Report lost or stolen equipment immediately to the Leadership Team
- Change all relevant account passwords if a device is lost or stolen
- Report suspected threats or security weaknesses to a Leader, or Online Safety Lead

Devices will be configured with the following minimum security controls:

- Password protection
- Full disk encryption
- Client firewalls
- Anti-virus / anti-malware software
- Automatic security updates
- Removal of unsupported or unrequired software
- Autorun disabled
- Minimal administrative accounts

9. Data Security

Elsley Primary School will take appropriate technical and organisational measures to reduce the risk of loss, unauthorised access, or disclosure of confidential data.

For the purposes of this policy, confidential data includes:

- Personally identifiable information as defined by the ICO
- Special Category personal data
- Unpublished financial information

Critical data and systems will be backed up regularly following the 3-2-1 backup methodology:

- 3 copies of data
- 2 different types of media
- 1 copy stored offsite or offline

Backups will be tested at least annually to ensure that restoration processes function effectively.

10. Sharing Files

Elsley Primary School recognises the security risks associated with sending and receiving confidential data. To minimise the risk of a data breach, users must:

- Consider whether an email may be a phishing attempt or whether a colleague's account may have been compromised
- Verify unusual financial requests, attachments or links through an alternative communication method
- Keep files on school-managed systems wherever possible
- Not send school files to personal accounts
- Verify recipients before sending confidential information
- Use file encryption where appropriate, sharing passwords or keys via separate communication channels
- Alert the Leadership Team or Online Safety Lead immediately of any suspected breach, malicious activity or scam. The Data Protection Officer will be notified where appropriate and will determine whether ICO notification is required.

11. Training

Elsley Primary School recognises that maintaining a high level of cybersecurity requires ongoing staff awareness and training.

The school will:

- Integrate cybersecurity training into INSET days
- Provide specialist training for staff responsible for IT systems
- Promote a 'no blame' culture to encourage prompt reporting of incidents
- Share regular reminders and updates via staff briefings

On a half-termly basis, the Leadership Team and/or Online Safety Lead will issue a phishing simulation test to staff. Those who do not successfully identify the phishing attempt will receive additional guidance or training.

12. System Security

The school's external IT support provider will incorporate security principles into the design and maintenance of IT services.

This includes:

- Security patching of network hardware, operating systems and software
- Proactive planning for hardware and software replacement before security support expires
- Active management of anti-virus systems
- Regular review and updating of existing security controls
- Segregation of wireless networks for visitors and personal devices from core school systems
- Risk assessment of new systems or projects prior to implementation

13. Major Incident Response Plan

The Cybersecurity Major Incident Response Plan forms part of the school's wider Business Continuity arrangements.

This includes identifying:

- Key decision-makers
- System impact assessments and restoration priorities
- Emergency procedures for operating without access to systems or data
- Alternative communication methods and contact lists
- Emergency financial authorisations
- External support agencies, including the IT support provider

14. Maintaining Security

Elsley Primary School recognises that the cost of recovering from a major cybersecurity incident can significantly exceed the ongoing investment required to maintain secure systems.

The school will therefore allocate appropriate resources to maintain secure infrastructure and minimise cyber-related risk.