Enfield County School for Girls

Cyber Security Policy

Respect, Responsibility, Co-operation, Equality and Generosity of Spirit

September 2026

Approved by:	Jennifer Gumbrell	**Date:**	March 2026
Last reviewed on:	September 2026		
Next review due by:	September 2027		

Contents

1. Introduction	3
2. Scope	3
3. Roles and Responsibilities	3
4. Technical Security Measures	3
5. User Account Management	4
6. Staff Training and Awareness	4
7. Exams and staff engaged to awarding organisations	4
8. Incident Response Plan	5
9. Disciplinary Action	5
10. Compliance and Auditing	6
Appendix 1	7
Appendix 2	8

1. Introduction

Enfield County School for Girls is committed to safeguarding its information assets, IT systems, and the personal data of students, staff, and stakeholders from cyber threats. This policy sets out our approach to cyber security, outlines roles and responsibilities, and ensures compliance with relevant UK legislation, including the Data Protection Act 2018, UK GDPR, and Keeping Children Safe in Education guidance.

2. Scope

This policy applies to all staff, students, governors who have access to Enfield County School for Girls IT systems and data.

3. Roles and Responsibilities

Role	Responsibilities
Head of Centre	Overall responsibility for policy implementation and cyber security strategy.
IT Manager/Team	Network Manager implements technical controls, monitors systems, responds to incidents, manages access and updates.
Data Protection Officer	Business Manager ensures compliance with data protection law, advises on data handling, and oversees data breaches.
All Staff	Follow this policy, complete annual training, report incidents or concerns promptly within the centre.
Governors	Oversee and review cyber security arrangements and policy compliance.
Students/Users	Use IT systems responsibly and report any concerns.

4. Technical Security Measures

Enfield County for Girls implements the following security measures, scaled to our size and needs:

- Firewalls and network security controls.
- Antivirus and anti-malware software on all devices.
- Regular software updates and patch management.
- Secure data backup and tested recovery procedures.

- Encryption for sensitive and personal data.
- Multi-factor authentication (MFA) for critical systems and remote access.
- Secure configuration and monitoring of cloud services (e.g. Office 365, MS Teams).
- Prompt removal of access for leavers.
- School devices are not compatible with USB storage devices.

5. User Account Management

- Staff receive annual training relating to cyber security including password governance.
- Password governance follows NCSC Guidance:
    - https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words
    - https://www.ncsc.gov.uk/collection/passwords/updating-your-approach
    - Access control and permissions are based on job roles and reviewed regularly.
    - Accounts are promptly disabled when users leave.
    - Account activity is monitored and audited.

6. Staff Training and Awareness

- All staff must complete annual cyber security training and annual refresher training, this includes:
    - School resilience to cyber attacks.
    - Who is behind cyber attacks?
    - Threats from outside and inside school. Please see Appendix 1 for examples.
    - Phishing awareness and social engineering defence training.
    - Setting strong passwords and keeping passwords safe.
    - Securing our school devices.
    - Calling out potential cyber threats or risks.
    - Exam Board login details - two factor authentication and keeping these login details safe.
    - Please see Appendix 2 for further information.

7. Exams and staff engaged to awarding organisations

- This policy recognises that strong cyber security is an integral responsibility for the successful and secure delivery of public examinations and this policy should be read alongside our Examination Suite of Policies which sets out in detail the response plan if there was a cyber-attack or failure in our ICT systems in order to mitigate impact on exams.
- All staff engaging with awarding organisation systems will undertake cyber security training annually. Staff are trained to ensure they set strong passwords for awarding organisations.
- Staff are not to share their login details for awarding organisations with anyone and to keep these login details safe.
- All staff with login details for awarding organisations are reviewed by the Exams Officer at least annually and when necessary to ensure permissions are based on job roles.

- Records of cyber security training are retained annually for all staff and will be available for inspection by JCQ.

8. Incident Response Plan

Any suspected or actual security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be reported immediately using the steps outlined below. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported using the steps below.

a. All staff members must immediately report any suspected or actual security incidents to the incident response team: Jen Foster (Deputy Headteacher) and Ediz Mehmet, Network Manager.
b. The incident response team will triage information. If an actual threat is identified then details of which will be escalated to the Headteacher and Data Protection Officer. The impact of the threat will be assessed and categorised and an incident manager will be assigned to lead on the response.
c. The response should contain or mitigate the impact of the threat and where possible eradicate the threat completely and recover data and systems.
d. A communication and reporting plan will be implemented to relevant stakeholders (staff, students, parents, governors, local authority, relevant awarding body, National Cyber Security Centre (NCSC).
e. A referral to awarding organisation(s) will be made when necessary in line with the process set out in our school's Examinations Malpractice Policy.
f. Post-incident review process: Conduct a review to identify lessons learned and update procedures if necessary.

9. Disciplinary Action

We expect all our staff to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal or written warning and train the staff on security.
- Intentional, repeated or large scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination.
- We will examine each incident on a case-by-case basis.

Additionally, staff who are observed to disregard our security instructions will face progressive discipline, even if their behaviour hasn't resulted in a security breach.

10. Compliance and Auditing

We will be working towards ensuring Enfield County School for Girls is cyber secure in line with the government's requirements by 2030.

- https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-core-standard

This policy will be reviewed annually by a member of the Senior Leadership Team and updated as necessary to reflect changes in technology, threats, and best practices.

Our data and ICT systems are reviewed annually or when necessary to reflect changes in technology, threats, and best practices.

Appendix 1

Threats A threat if left unchecked, it could disrupt the day-to-day operations of the school, the delivery of education and ultimately has the potential to compromise local and national security.

Types of Threats

a) Cybercriminals and Cybercrime

Cybercriminals are generally working for financial gain. Most commonly, for the purposes of fraud: either selling illegally gained information to a third party, or using directly for criminal means. Key tools and methods used by cybercriminals include:

- Malware - malicious software that includes viruses, Trojans, worms or any code or content that could have an adverse impact on organisations or individuals.
- Ransomware - a kind of malware that locks victims out of their data or systems and only allows access once money is paid.
- Phishing - emails purporting to come from a public agency to extract sensitive information from members of the public.

b) Hacktivism Hacktivists will generally take over public websites or social media accounts to raise the profile of a particular cause. When targeted against local government or school websites and networks, these attacks can cause reputational damage locally. If online services are regularly disrupted by cyber-attacks this could lead to the erosion of public confidence in using such services. Hacktivist groups have successfully used distributed denial of service (DDoS - when a system, service or network is burdened to such an extent by an electronic attack that it becomes unavailable) attacks to disrupt the websites of a number of councils already.

c) Insiders Staff may intentionally or unintentionally release sensitive information or data into the public domain. This may be for the purpose of sabotage or to sell to another party, but more often than not is due to simple human error or a lack of awareness about the particular risks involved.

d) Zero-day threats. A zero-day exploit is a cyber-attack that occurs on the same day a weakness is discovered in software. At that point, it's exploited before a fix becomes available from its creator. It is an attack that exploits a previously unknown security vulnerability. This poses a risk to any computer or system that has not had the relevant patch applied, or updated its antivirus software.

e) Physical threats. The increasing reliance on digital services brings with it an increased vulnerability in the event of a fire, flood, power cut or other disaster, natural or otherwise, that impacts upon our IT systems.

f) Terrorists. Some terrorist groups demonstrate intent to conduct cyber-attacks, but fortunately have limited technical capability. Terrorist groups could obtain improved capability in a number of ways, namely through the sharing of expertise in online forums providing a significant opportunity for terrorists to escalate their capability.

g) Espionage. Several of the most sophisticated and hostile foreign intelligence agencies target UK government and public sector networks to steal sensitive information. This could ultimately disadvantage the UK in diplomatic or trade negotiations, or militarily.

Appendix 2

Staff are trained annually to prevent a cyber-security attack and this training is updated annually in response to changes in technology and best practice.

Some examples are shown below.

Protect personal and school devices
In general, staff should try to only use school-issued devices to access school emails, accounts or folders. When staff use personal digital devices to access school emails or accounts, they introduce a security risk to our data.

We advise our staff to keep both their personal and school-issued computer, tablet and mobile phone secure. They can do this if they:

- Keep all devices password protected.
- Ensure that the school-installed antivirus software (ESET) is installed on their school owned computer and that they have antivirus software installed on home computers/devices.
- Ensure they do not leave their devices exposed or unattended.
- Ensure that school-wide security updates of browsers and systems have taken place.
- Log into school accounts and systems through secure and private networks only.

We also advise our staff to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new staff receive school-issued equipment they will receive instructions for password management setup.

Antivirus / anti-malware software is installed on all school-owned laptops / devices and we advise all staff to have antivirus software installed on their own devices

Keep emails safe
Emails often host scams and malicious software (e.g. worms). To avoid virus infection or data theft, we instruct staff to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing").
- Be suspicious of clickbait titles (e.g. offering prizes, advice).
- Check email address and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks).

Manage passwords properly
Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they cannot be easily hacked, but they should also remain secret. For this reason, we advise our staff to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays).

General guidance on creating a password is to take three random words and to add a number and a special character - e.g. DinosaurStarRose14%.

- Remember passwords instead of writing them down. If staff need to write their passwords, please keep passwords and identifiers separate or, at least, secure.
- Exchange credentials only when absolutely necessary. When exchanging them in person is not possible, staff should prefer the phone instead of email, and only if they personally recognise the person they are talking to.

Transfer data securely

Transferring data introduces security risk. Staff must:

- Avoid transferring sensitive data (e.g. customer information, staff records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request staff to ask our IT provider (PEL) for help.
- Share confidential data over the school network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.
- Ensure that data is sent to the correct email address/contact and take particular care when sending mass emails (e.g. via Bcc - Blind Carbon Copy - facility).
- Report scams, privacy breaches and hacking attempts, following this policy.