Children First Learning Partnership
Cyber Security Policy

(Version 2)

The Cyber Security / Online Safety Policy in respect of the Children First Learning Partnership has been discussed and adopted by the Directors Board	
Chair of Board:	*Mrs N Chell*
Responsible Officer:	*CEO – Mrs A Rourke*
Agreed and ratified by the Directors Board on:	*06/07/2026*
To be reviewed: *July 2027*	

The Children First Learning Partnership reviews this policy annually. The directors may, however, review the policy earlier than this, if the Government introduces new regulations, or if the Trust receives recommendations on how the policy might be improved

Contents

1. Introduction

This policy is to be read in conjunction with the School Safeguarding, AI policy, GDPR and Acceptable Use Policy. Appendix 1 is a cyber security quick guide for staff.

A cybersecurity incident can have a major impact on any organisation for extended periods of time. For a school, this can range from minor reputational damage and the cost of restoring systems from existing backups, to major incidents such as losing student work or access to learning platforms and safeguarding systems, which could lead to data-protection fines or even failing an inspection. This Cybersecurity Policy outlines the Children First Learning Partnership guidelines and security provisions which are there to protect our systems, services and data in the event of a cyberattack.

2. Scope Of Policy

This policy applies to all Children First Learning Partnership staff, contractors, volunteers and anyone else granted permanent or temporary access to our systems and hardware. It also covers the physical and technical elements that are used to deliver IT services for the school.

3. Cyber Essentials

The Children First Learning Partnership supported by Evolve IT support have completed the cyber essentials certifications and will maintain and review the Cyber Essentials certification annually.

4. Risk Management

The Children First Learning Partnership will include cyber security risks on its organisational risk register, regularly reporting on the progress and management of these risks to Trustees annually. Artificial Intelligence (AI) is an emerging cyber risk including Phishing and social engineering, Deepfake audio / visual impersonation, synthetic identity fraud and AI -generated malware or prompt-based data leakage. AI risks are reviewed alongside other cyber threats on the trust risk register, in line with the AI policy's monitoring expectations

5. Physical Security

The Children First Learning Partnership ensure there is appropriate physical security and environmental controls protecting access to its IT Systems, including but not limited to lockable cabinets, and secure server/communications storage.

6. Asset Management

To ensure that security controls to protect the data and systems are applied effectively, The Children First Learning Partnership with support from Evolve IT will maintain asset registers for, files/systems that hold confidential data, and all physical devices (servers, switches, desktops, laptops etc) that make up its IT services

All AI tools must be approved through the CFLP AI tool approval process and appear on the AI register. AI tools are treated as information systems, not apps, and fall under asset management,

security configuration and risk assessment. Unapproved AI tools are considered an unauthorised system risk.

7. User Accounts

Users are responsible for the security of their own accounts. If at any time they believe their credentials may have been compromised, for example after a phishing scam, they must change their password and inform the Evolve IT Service Desk as soon as possible. Personal accounts should not be used for work purposes. Personal AI accounts for school business or shared AI logins are not to be used. AI credentials are high risk accounts due to data-extraction and impersonation risks. The Children First Learning Partnership will implement multi-factor authentication where it is practicable to do so.

8. Devices

To ensure the security of all Children First Learning Partnership Trust issued devices and data, users are required to:

• Lock devices that are left unattended

• Update devices when prompted

• Report lost or stolen IT equipment as soon as possible to the Evolve IT Service Desk

• Change all account passwords at once when a device is lost or stolen (and report immediately to the Evolve IT Service Desk

• Report a suspected threat or security weakness in Children First Learning Partnership Trust's systems to Evolve IT Service Desk and SLT

Children First Learning Partnership Devices will be configured with the following security controls as a minimum:

• Password protection

• Full disk encryption

• Client firewalls

• Anti-virus / malware

• Automatic security updates

• Removal of unrequired and unsupported software

• Autorun disabled

• Minimal administrative accounts

9. Data Security

The Children First Learning Partnership will take appropriate measures to reduce the likelihood of the loss of availability to, or the disclosure of, confidential data.

The Children First Learning Partnership defines confidential data as:

• Personally identifiable information as defined by the ICO

• Special Category personal data as defined by the ICO

• Unpublished financial information

Critical data and systems will be backed up on a regular basis following the 3-2-1 backup methodology

• 3 versions of data

• 2 different types of media

• 1 copy offsite/offline

Personal, identifiable, or confidential data must never be entered into generative AI systems.

10. Sharing Files

The Children First Learning Partnership recognises the security risks associated with sending and receiving confidential data. To minimise the chances of a data breach users are required to:

• Consider if an email could be a phishing email or that a colleague's account could be 'hacked'. If something does not feel right check with the sender by another method, particularly in relation to financial transactions, attachments, or links to websites

• Wherever possible, keeping Children First Learning Partnership on school systems

• Not sending school files to personal accounts

• Verifying the recipient of data prior to sending

• Using file encryption where possible, sending passwords/keys via alternative communication channels

• Alerting [IT Support/DPO/SLT] to any breaches, malicious activity or suspected scams for action as appropriate

• Treat AI upload misuse as a data breach incident

11. Training

The Children First Learning Partnership recognises that it is not possible to maintain a high level of Cybersecurity without appropriate staff training. It will integrate regular Cybersecurity training and AI training into Inset days, provide more specialist training to staff responsible for maintaining IT systems and promote a "No Blame" culture towards individuals who may fall victim to sophisticated scams.

12. System Security

Evolve IT support will build security principles into the design of IT services for the Children First Learning Partnership but not limited to:

• Security patching – network hardware, operating systems and software

• Pro-actively plan for the replacement of network hardware, operating systems and software before vendors stop providing security support for them

• Actively manage anti-virus systems

• Actively manage and test backups

• Regularly review and update security controls that are available with existing systems

• Segregate wireless networks used for visitors' & staff personal devices from school systems

• Review the security risk of new systems or projects

- Regular review of embedded AI features in SaaS platforms

13. Major Incident Business Continuity Plan

The Children First Learning Partnership will develop, maintain, and regularly test a Cybersecurity/ AI Business Continuity Plan. This will include identifying or carrying out:

• Key decision-makers

• Key system impact assessments and restoration priorities (i.e. which backups needs to be restored first for the school to become operational again)

• Emergency plans for the school to function without access to systems or data

• Alternative methods of communication, including copies of contact details

• Emergency budgets and who can access them / how

• Key agencies for support (e.g. IT support company)

14. Maintaining Security

The Children First Learning Partnership understands that the financial cost of recovering from a Major Cybersecurity Incident can far outweigh the ongoing investment in maintaining secure IT systems. The Children First Learning Partnership will budget appropriately to keep cyber related / AI risk to a minimum. There will be an annual review of the Cyber security policy and AI policy.

15. Appendix 1

Cyber Security Quick Guide (Staff)

This quick guide summarises the minimum day-to-day actions staff must follow to protect Children First Learning Partnership systems and data. It sits alongside this Cyber Security Policy, the Acceptable Use Policy, Safeguarding, GDPR and the AI Policy.

If you suspect a breach, scam or cyber incident (act immediately)

Stop: do not click further, reply, forward, or continue entering information.

Isolate (if safe): disconnect the device from Wi-Fi/Ethernet (airplane mode). Leave it switched on.

Report immediately: contact **Evolve IT Service Desk**. If personal data may be involved, also notify the **DPO**. If there is any safeguarding concern, also notify the **DSL/SLT**.

Preserve evidence: keep the email/message, take screenshots if helpful, and note the time, what happened, and what information may be affected.

Do not self-fix: do not reset devices, delete evidence, or run unapproved tools unless instructed by IT.

Reportable examples include: clicking a suspicious link/attachment; entering your password on an unexpected page; unexpected MFA prompts; device lost/stolen; suspicious sign-in alerts; antivirus/malware warnings; mis-sent emails containing personal/confidential data; or any upload of school/personal/confidential data into an unapproved AI tool.

Email, phishing and financial scams

Think before you click: be cautious with unexpected links, attachments, QR codes, or requests to login.

Verify by another method: if an email request feels unusual (especially urgent), confirm using a known phone number or in-person.

Payments/bank details: never change supplier bank details or approve unusual payments based on email alone—use a second-channel check.

Do not forward suspicious emails to colleagues—report them to Evolve IT Service Desk.

Passwords and multi-factor authentication (MFA)

Minimum password length: at least **[12]** characters (use a long passphrase). Do not reuse Trust passwords on other websites.

Change your password immediately if you think it may be compromised, and report it to Evolve IT Service Desk.

MFA: enable and use MFA where provided (Trust accounts and systems). Never approve an MFA prompt you did not initiate.

No shared accounts: do not share logins or use personal accounts for Trust work. Do not use personal AI accounts or shared AI logins for school business.

Device security and physical security

Lock your screen whenever you step away, even briefly.

Do not leave devices unattended in classrooms, corridors, halls, reception areas, or vehicles.

Store devices securely in locked cupboards/trolleys/rooms when not in use.

Lost or stolen device: report immediately to Evolve IT Service Desk and follow IT instructions (including password resets where required).

Do not connect unknown USB devices to Trust equipment.

Data handling and sharing files

Keep work on Trust systems: avoid sending school files to personal email or storing them in personal cloud accounts.

Check recipients before sending, especially when emailing personal/confidential data.

Use approved sharing methods and follow encryption/password guidance where instructed (send passwords via a different channel).

AI data rule: never upload personal, identifiable, or confidential data into public AI chatbots or consumer AI services. If this happens, treat it as a data breach and report immediately.

Remote working (if applicable)

Use Trust-managed devices and Trust accounts wherever possible.

Avoid working on confidential information in public spaces where screens can be overlooked.

Do not use public/shared computers for Trust systems.

Report immediately if you believe your device, account, or data may have been exposed.

Need help or unsure? Report it. The Trust promotes a no-blame culture: early reporting helps protect pupils, staff and systems.

Version Control:

Version	Date	Amendment	By
V1	28.08.2025	New Policy	OM
V2	11.05.2026	Amended to reflect the inclusion to reference the AI policy and appendix 1 added as a staff quick guide	OM