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.