Cyber Security Statement and Policy

Frobel Education's Executive Board oversee policy and procedure for its educational services:

Last Reviewed: September 2026

By: Executive Board

Date of next review: September 2027

This Cyber Security Policy outlines the guidelines and procedures for ensuring the security and privacy of digital systems, networks, and data within Frobel Education. It aims to protect the confidentiality, integrity, and availability of information, prevent unauthorised access and malicious activities, and promote responsible and safe digital practices.

This policy applies to all staff, learners and other individuals granted access to Frobel Education's digital resources and networks.

All users must adhere to Frobel Education's procedures and policy and respect all applicable laws, regulations, and copyrights when using Frobel Education's digital resources and use digital resources for educational purposes and in accordance with Frobel Education policies.

Storage servers are physically stored and maintained on site. Data stored locally does not enter the 'cloud' or leave the site. Staff do not remotely access the data in any way in order to provide greater levels of security by minimising the potential for hackers to enter the network.

Cloud services are used for some databases (Sims, etc) although these are all protected behind firewalls as well as 2FA login systems.

In the event of any form of network attack, the CEO and Network Manager will be informed immediately and the Deputy CEO will inform the DPO, Judicium, to agree next steps and potential ICO involvement and reporting.

The Role of the Executive Board

The Executive Board (EB) is responsible for setting policy and procedure and for putting in place processes and procedures that ensure all Elements are Compliant and that staff are fully trained and competent in managing cyber threats and risks well.

Frobel Education EB maintains up to date privacy policies and procedures in compliance with applicable privacy laws and regulations.

The EB will review this policy annually and update as needed to address emerging cyber threats or changes in regulations.

The Executive Board delegates operational management of Cyber Security to the ***Finance, Premises, IT, Staffing and Risk Management Committee.*** This is set out on Frobel Education's Organisational Chart 2024-2025.

The Role of the Management Committee

The Management Committee Chair will promptly investigate reported incidents, take necessary actions to mitigate risks, and document the response process.

The IT Management Committee Chair will ensure timely communication will be maintained with affected parties, as appropriate, during security incidents.

The Management Committee will arrange termly checks, scrutiny and assessments to ensure compliance with this policy.

The Management Committee arranges the DFE Digital Standards Audit to be completed annually and this informs the 'cyber security' sections of the Risk Register and Business Continuity Plan.

The IT Management Committee presents a termly report to the Executive Board.

The Role of the Network Manager

The Network Manager regularly backs up data and store backups securely in the organisation's safe.

The Network Manager and/or Website and Social Media Manager will maintain up-to-date software, firmware, and operating systems on all devices connected to Frobel Education's network.

The Network Manager and/or Website and Social Media Manager will regularly install security patches and updates.

The Network Manager Secure wireless networks with strong encryption and authentication mechanisms and segregates guest networks from internal networks.

The Network Manager implements secure remote access protocols and the use of virtual private networks (VPNs) when accessing the Frobel Education's network from external locations.

The Role of the DSL

The DSL takes lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems in place).

The DSL will train and support staff – on matters of safety, safeguarding and welfare (including online and digital safety); when deciding whether to make a referral by liaising with relevant agencies; and as a source of safeguarding support, advice and expertise for all staff.

The DSL will ensure risks associated with being online are assessed and mitigated and complete associated risk assessment/s.

The DSL will ensure that staff understand the risks associated with being online (and the additional risks faced by vulnerable learners) and know how to keep learners safe while they're online at school and recognise the additional risks that learners with SEND face online, and know how to support them to stay safe online.

To manage their role effectively, the DSL will understand relevant data protection legislation, especially the Data Protection Act 2018 and the UK General Data Protection Regulation.

Operational Processes and Procedures

The FE network organises its information and data on network drives set up for specific staff access, depending on staff role. Staff have access only to information and data that is required to carry out their professional duties. Learners do not have access to staff drives.

HR documents are stored on the 'management' drive, accessed only by Central Service senior staff and senior leaders and are also encrypted with passwords, known only to the CEO, Deputy CEO and Chair of the appropriate Management Committee.

All Exams' data is held internally and is never managed or worked on outside of Frobel Education buildings.

It is not permitted for staff to work on sensitive or personal data outside of Frobel Education buildings.

SIMS and Management Systems are managed only in Frobel Education buildings.

Social Media accounts are set up with 2 factor authentication.

Bank accounts are set up with 2 factor authentication.

Multi-factor authentication will be put in place wherever possible.

Outsourced Business and SLAs

All companies, to whom Frobel Education outsources workflows, have been scrutinised via our due diligence process and have undergone a GDPR DPIA that is signed off by the DPO.

Server 20i hosts the organisation website and has a robust cyber security policy and good record of safety and security.

Frobel Education website, social media accounts and e-commerce shop are managed and run by Greynoise Ltd: a company with more than 10 years' experience and a good history of effective and safe cyber security. DPIAs are completed for Greynoise and due diligence has been completed to explore their policy and procedures in relation to cyber security.

Instructions for Staff

Laptops must be kept locked in car boots when they are travelling home with senior leaders. They must then be kept safely and securely at home.

Staff must set their devices to revert to 'lock' mode after 1 minute of inactivity.

Staff must handle sensitive and confidential information responsibly, ensuring appropriate access controls and encryption when necessary and follow policy as set out in policy documents and the Staff handbook.

USBs are not permitted to transfer information.

All staff must protect personal login credentials and report any suspected or actual security breaches promptly as per staff training and staff briefing information.

Staff will only access the Frobel Education's network and resources using their authorised accounts.

Staff are to change their password every half term.

All staff must promptly report any suspected or actual security incidents, including unauthorised access, data breaches, or malware infections, to the CEO, Mr Khan, or Deputy CEO Mrs Bower, who will inform the Network Manager and DPO.

Staff will only collect, store, and process personal data only for legitimate educational purposes.

Senior leaders will ensure appropriate security controls, including encryption, when handling personal data.

HR Central Services will obtain consent from individuals as required by relevant privacy laws.

Violations of this policy may result in disciplinary action, including but not limited to temporary or permanent loss of network privileges, termination of employment, or legal consequences, depending on the severity of the violation and applicable laws. Any concerns or suspected policy violations should be reported to the CEO or designated authorities.

Staff Training

All staff receive training in cyber security awareness. They attend a staff briefing, that trains in the following 3 areas:

- ✓ **Poor password security:** easy to guess, written down somewhere, or shared with people
- ✓ **Harmful links in emails:** usually disguised to appear innocent, these links can forcefully download malicious software ('malware') or take you to a seemingly legitimate webpage that will steal your password or personal data
- ✓ **Malware:** malicious software, disguised as a legitimate piece of software, that will damage your computer or steal information (such as passwords and personal data)

Frobel Education has a monthly colleague newsletter that features cyber awareness updates.

By adhering to this Cyber Security Policy, we can collectively contribute to maintaining a secure and protected digital environment within Frobel learning.

Appendix A

Links to other Frobel Education documents and policies

Risk Assessment and Audit, a summary

The organisation's risk assessment and audit identified the following potential risks that are mitigated through implementation of this policy and its procedures.

Information Security

Information security breach might include:

- The theft and unauthorised access to significant confidential information, for example exam papers
- guidance, standards and policy documents
- the unauthorised access to personal information, for example bank and credit card details, health records

Cyber security

A cyber security incident might include malicious software execution resulting in:

- outages
- data loss
- costs incurred to recover associated data and access to the system

Preventative measures included in our policy and procedures include:

- ensuring all software and devices have security patches applied regularly, including anti-virus, which should be automated and only use software and operating systems that are supported
- ensuring the network is securely configured, turn on firewalls and follow best practice for end user devices
- performing regular data backups, ensuring they are stored independently and/or appropriately protected

- understanding your reliance on IT and have a business continuity plan to enable you to operate without it
- regularly review policies to ensure cyber security standards are maintained
- implementing content filtering to prevent inappropriate content access
- verify email senders, do not circumvent your security processes
- having effective policies to educate staff and learners on cyber security