The Eliot Bank and Gordonbrock Schools Federation

Cybersecurity

Author:	Tony Hardy-Hall	Date:	September 2023
Approved by:	Governing Body	Date:	September 2023
Issue Date:	September 2024	Next Review Date:	September 2025

1. Key people

Executive Headteacher (EB/GB) & Head of School (EB) **Head of School (GB)**	Maria Gilmore Jane Wright
Chair of Governors	Peter Fidel
Network manager / other technical support	Deku Solutions Ltd
Date this policy was reviewed and by whom	September 2023, Tony Hall
Date of next review and by whom	September 2024, Tony Hall

2. Overview

2.1 Aims

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 Gordonbrock and Eliot Bank Schools Federation guidelines and security provisions which are there to protect our systems, services and data in the event of a cyberattack.

2.2 Scope

This policy applies to all Gordonbrock and Eliot Bank Schools Federation 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. Risk management

Risk management, including cybersecurity risks, is an agenda item for Resources Governors, who meet at least three times a year.

4. Physical security

Gordonbrock and Eliot Bank Schools Federation will ensure there are appropriate physical security and environmental controls protecting access to its IT Systems, including but not limited to lockable cabinets and secure server/communications rooms.

5. Asset management

To ensure that security controls to protect the data and systems are applied effectively, Gordonbrock and Eliot Bank Schools Federation will maintain asset registers for all physical devices (servers, switches, desktops, laptops etc) that make up its IT services.

6. 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 Head of School. as soon as possible. Personal accounts should not be used for work purposes. Gordonbrock and Eliot Bank Schools Federation will implement multi-factor authentication for staff with access to significant datasets (e.g. LGFL logins, CPOMS), where possible.

7. Devices

To ensure the security of all Gordonbrock and Eliot Bank Schools Federation issued devices and data, users are required to:

- Lock devices that are left unattended
- Update devices when prompted
- Report lost or stolen equipment as soon as possible to the Head of School
- Change all account passwords at once when a device is lost or stolen (and report immediately to the Head of School

- Report a suspected threat or security weakness in Gordonbrock and Eliot Bank Schools Federation systems to the Head of School

Devices will be configured with the following security controls as a minimum:

- Password protection
- Full disk encryption
- Client firewalls
- Anti-virus / malware software [eg Sophos and Malwarebytes for LGfL schools – see sophos.lgfl.net / malwarebytes.lgfl.net]
- Automatic security updates
- Removal of unrequired and unsupported software
- Autorun disabled
- Minimal administrative accounts

8. Data security

Gordonbrock and Eliot Bank Schools Federation will take appropriate measures to reduce the likelihood of the loss of availability to, or the disclosure of, confidential data.

Gordonbrock and Eliot Bank Schools Federation 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.

9. Sharing files

Gordonbrock and Eliot Bank Schools Federation 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 Gordonbrock and Eliot Bank Schools Federation files 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 (e.g. LGFL's USO FX)
- Alerting [IT Support/DPO] to any breaches, malicious activity or suspected scams

10.Training

Gordonbrock and Eliot Bank Schools Federation recognises that it is not possible to maintain a high level of Cybersecurity without appropriate staff training. It will integrate regular Cybersecurity 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.

11.System security

Deku Solutions Ltd. will build security principles into the design of IT services for Gordonbrock and Eliot Bank Schools Federation. These include:

- Security patching – network hardware, operating systems and software
- Proactively 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

12.Major incident response plan

Gordonbrock and Eliot Bank Schools Federation will develop, maintain, and regularly test a Cybersecurity Major Incident Response 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)

13.Maintaining security

Gordonbrock and Eliot Bank Schools Federation understands that the financial cost of recovering from a Major Cybersecurity Incident can far outweigh the ongoing investment in maintaining secure IT systems. Gordonbrock and Eliot Bank Schools Federation will budget appropriately to keep cyber-related risk to a minimum.