Edinburgh College

Corporate Ref.	FEIT 003
Level	3
Senior Responsible Officer	Chief Executive Officer
Version	2
EIA	N/A
Approved by	Chief Executive Officer
Approved date	3 June 2024
Superseded version	1
Review date	3 June 2025

Network Security Policy

Version Control

Version	Author	Date	Changes
2	Digital Infrastructure Service Lead	27/05/2024	Moved to new template and narrative updated.

1. INTRODUCTION AND POLICY AIM

This document defines the Network Security Policy for Edinburgh College. The Network Security Policy applies to all network hardware, services on the network and network attached systems.

For the purpose of this policy a network is defined as Edinburgh College's connected (physically and wirelessly) data network that allows computing devices (including phones) to exchange data.

The aim of this policy is to ensure the security of the network. To facilitate this, the College will:

- Protect assets against unauthorised access or disclosure **(Confidentiality).**
- Protect the network from unauthorised or accidental modification and ensure the accuracy and completeness of data assets **(Integrity)**.
- Ensure the network is accessible how and when users need it **(Availability).**

2. POLICY OBJECTIVES

The objectives of this policy are:

- To protect all hardware, software, and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures.
- To provide effective protection that is commensurate with the risks to the College's network assets.
- To implement the policy and associated procedures in a consistent, timely and cost-effective manner.
- To ensure the College is compliant with all relevant legislation, including (but not limited to):
    - UK Data Protection Act 2018
    - UK General Data Protection Regulation (UK GDPR)
    - Computer Misuse Act 1990

- Human Rights Act 1998
- Freedom of Information Scotland Act 2002
- Electronics Communications Act 2000
- Copyright, Designs and Patents Act 1988

3. PHYSICAL AND ENVIRONMENTAL SECURITY

Network equipment (principally routers, switches, and servers) shall be housed in a controlled and secure environment. Critical or sensitive network equipment will be housed in an environment that is monitored for temperature, humidity, and power supply quality.

Critical or sensitive network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.

Critical or sensitive network equipment will be protected from power supply failures and protected by intruder alarms and fire suppression systems.

Eating and drinking is forbidden in areas housing critical or sensitive network equipment.

All visitors to secure network areas must be authorised by an appropriate manager.

All visitors to secure network areas must be made aware of network security requirements.

The movement of visitors to secure network areas must be recorded. The log will contain name, organisation, purpose of visit, date, and time in and out.

The Digital Infrastructure Service Lead, or appropriate deputy, shall ensure that all relevant staff are made aware of procedures for visitors and that visitors are escorted when necessary.

4. ACCESS CONTROL TO THE NETWORK

Access to limited-access network services shall be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access. Remote access to the network will be via the College’s remote access software.

Departmental business managers will approve user access to systems including network access via standard staff joiner/leaver processes.

Access rights to network services will be allocated on the requirements of the user's role, rather than on a status basis.

All users of network services will have their own individual user identification and password.

Users are responsible for ensuring their password is kept secret (please refer to the College’s IT Facilities Acceptable Use Policy for further details).

User access rights shall be removed or reviewed for those users who have left the College or changed roles as soon as practically possible.

5. THIRD PARTY ACCESS CONTROL TO THE NETWORK

Third party access to network systems, services, hardware, and network attached systems shall be based on a formal contract that satisfies all necessary security conditions.

All third-party access to network systems, services, hardware, and network attached systems must be logged.

6. MAINTENANCE AND FAULT MANAGEMENT

The Digital Infrastructure Service Lead will ensure that adequate maintenance contracts are maintained and periodically reviewed for all network equipment.

The Digital Infrastructure Service Lead is responsible for ensuring that a log of all faults on network systems and equipment is maintained and reviewed.

Edinburgh College shall ensure that timely information regarding the technical vulnerabilities of information systems is obtained. Any vulnerability will be assessed and any risks will be appropriately controlled.

The use of privileged utility programs that may be capable of overriding system and application controls will be controlled and restricted.

Operational software shall only be installed by authorised system administrators and authorised third parties (see section 5).

7. NETWORK OPERATING PROCEDURES

Documented operating procedures should be prepared for the operation of network services and systems, to ensure their correct, secure operation.

Changes to operating procedures must be authorised by the Digital Infrastructure Service Lead.

8. DATA BACKUP AND RESTORATION

The Digital Infrastructure Service Lead is responsible for ensuring that backup copies of network configuration data are taken regularly.

Documented procedures for backup processes and storage will be produced and communicated to all relevant staff.

9. USER RESPONSIBILITIES, AWARENESS AND TRAINING

The College will ensure that all users of network systems, services, hardware, and network attached systems are provided with the necessary security guidance, awareness and, where appropriate, training to discharge their security responsibilities.

All users of network services and systems must be made aware of the contents and implications of the Network Security Policy and IT Facilities Acceptable Use Policy.

All users must ensure that they protect the network from unauthorised access. They must log off the network when finished working.

Irresponsible or improper actions by users may result in disciplinary action.

10. PROTECTION AGAINST MALWARE

Software to protect against malware should be installed on all client devices including mobile computing assets.

Software used to protect College systems against malware shall be regularly reviewed and updated.

Procedures on dealing with malware protection and attacks shall be developed and documented together with appropriate business continuity plans.

11. CLOCK SYNCHRONISATION

All network systems and services shall be synchronised.

12. LOGGING AND MONITORING

12.1 Logs to be Collected

Adequate event logs recording network activity, exceptions, faults, and information security events shall be produced, kept, and regularly reviewed. The requirements for audit logging at the College include:

Network Activity Logs

These logs should capture details of traffic passing through the college firewalls, including source and destination IP addresses, ports, protocols, and the volume of data transferred.

Exception Logs

Logs that record any deviations from normal operations or error conditions in the system. Examples include application error logs, system error logs, and logs from intrusion detection systems.

Security Event Logs

These logs should capture security-related events such as failed login attempts, account lockouts, privilege escalation attempts, and antivirus alerts. Logs from security information and event management (SIEM) systems, anti-malware software, and access control systems are examples.

Application Logs

Record application-specific events, such as user activities, application errors, transaction histories, and access to sensitive data. Examples include logs from learning management systems, student information systems, and financial applications.

12.2 Scope of Logging

Critical Systems

Systems and applications which are critical to the College's operations must have comprehensive logging enabled. This includes systems that handle sensitive data (e.g., financial systems, student information systems) and systems crucial for daily operations (e.g., email servers, learning management systems).

Data Sensitivity

Systems that contain sensitive data must have detailed logging to track access and modifications to this data. Examples include databases containing personal information, health records, and financial data.

System Exposure

The exact level of logging required depends on the details of the specific system, but systems which are directly exposed to the internet or other external networks require more stringent logging due to higher risks of attack. Internal systems may have less rigorous logging based on their exposure level but still require adequate monitoring.

12.3 Log Review

To manage the log review process effectively, the College should employ automated log analysis using Security Information and Event Management (SIEM) systems to aggregate and analyse logs from different sources, flagging suspicious activities and generating alerts. Machine learning algorithms should be used to detect anomalies in log data that may indicate potential security threats. The SIEM system must be configured to prioritise alerts based on severity, ensuring that the most critical issues are reviewed promptly.

Additional scheduled manual reviews are appropriate for high-risk or sensitive systems, such as financial systems, student information systems, and systems handling personal data.

12.4 Log Retention

Logs must be retained for a sufficient period to allow for thorough investigations and audits while balancing storage constraints and the resulting costs. The following table outlines the retention periods for different types of logs used within the College.

Logs need to be stored in a separate system to ensure availability in case of compromise.

Type of Log	Description	Retention
Network Activity and Firewall Logs	Logs capturing details of all network traffic, including IP addresses, ports, protocols, data volumes, and traffic passing through the firewall.	90 days
Exception Logs	Logs recording deviations from normal operations or error conditions in systems and applications.	90 days
Fault Logs	Logs documenting hardware or software faults, including	90 days

	server crashes and network device malfunctions.	
Security Event Logs	Logs capturing security-related events such as failed login attempts, account lockouts, and antivirus alerts.	90 days
Application Logs	Logs recording application-specific events, such as user activities, application errors, and transaction histories. Depending on the application, a longer retention period may be necessary.	90 days or longer
Privileged User Activity Logs	Logs detailing the actions of users with elevated permissions, including system configuration changes and access to sensitive data.	90 days
Microsoft Entra ID Logs	Logs capturing activities and changes in Microsoft environments, including user and admin actions.	90 days
Azure Activity Logs	Logs capturing actions and changes within Azure resources and services.	90 days
Office 365 Activity Logs	Logs recording activities and changes in Office 365 applications and services.	90 days
MFA Authentication and Administration Logs	Logs recording multi-factor authentication events and administrative actions related to MFA.	90 days
Server Common Event Logs	General logs from server systems, capturing system events and status changes.	90 days
PAM Logs	Privileged Access Management logs capturing	90 days

	activities and access events related to privileged accounts.	

13. POLICY REVIEW

This Policy will be reviewed and updated every three years, or as required to ensure that the policy remains aligned with changes to relevant laws, contractual obligations, and best practice.

End of document