Policy Number	FEIT 003
Level	3
Issue	1
Issue Date	07/12/2020
Review Date	15/10/2023
Author	A. Williamson
SMT approval	15/10/2020

Edinburgh College

For the future you want

Network Security Policy

Estates Services & IT

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):

- The Data Protection Act 2018
- The General Data Protection Regulation (2016)
- 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

Adequate event logs recording network activity, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

Logging facilities and log information shall be protected against tampering and unauthorised access.

The activity of privileged users shall be logged and the logs protected and regularly reviewed.

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.