Policy Number	FEIT 004
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

Physical and Environmental Security Policy

Estates Services & IT

1. OBJECTIVE

To prevent unauthorised access or damage to IT systems or services. To prevent the loss of, damage to, or compromise of information assets, and interruption to the business activities of the College.

2. POLICY REQUIREMENTS

All computer equipment that provides access to College information should be kept secure by physical means or by using good practice (this is especially important for users of mobile devices).

File servers and equipment that store or process key information or high availability data shall be located in physically secured areas.

Entry to secured areas will be restricted to authorised users:

- Employees of the College will have their cards encoded with the access rights approved by their line manager and the Chief Operating Officer.
- Employees must not lend their card to anyone, or allow anyone to follow them through card-controlled doors (tailgating).
- Access rights will be revoked immediately for staff who leave the employment of the College.
- Other visitors will be granted access for specific and authorised purposes only, and will be supervised.
- A log will be maintained of all access to restricted areas, via the signing out of access keys and the entry card system logs.

3. CABLING BETWEEN BUILDINGS

Cables between buildings should be underground wherever possible. Ducts and entry points into buildings should be secure and inspected annually for signs of damage or interference. A log of these inspections will be retained by the Head of Estates Services and Estates Services managers.

4. INTERNAL CABLING

Wherever possible, cabling within buildings should be installed in ceiling voids and secure ducts.

5. WIRELESS ACCESS POINTS

Wherever possible, wireless access points should be installed at a high level to make them less exposed and more secure from theft or tampering.

6. COMMUNICATIONS RACKS AND WIRING CABINETS

All communications equipment will be kept secure, either in locked rooms or in racks and cabinets with locks. Keys to communications and/or server rooms, racks and cabinets will be held securely by technical specialists and the College's Security Service so that they are not available to individuals who are unauthorised to access network devices.

7. ENVIRONMENTAL CONTROLS

Data centres will be protected by appropriate air conditioning and very early smoke detection systems. Temperatures in data centres will be monitored by Operations staff, and undue variances reported immediately to the College's Estates Department.

Equipment will be protected from power failures or electrical anomalies. Data centres will be protected by suitable local stand-by power supplies (generator or uninterruptible power supply).

Wiring cabinets, and the rooms in which they are located, should be inspected annually to assess security risks and hazards arising from environmental conditions. A log of these inspections will be retained by the Head of Estates Services and Estates Services managers.

8. EQUIPMENT MAINTENANCE

Equipment will be maintained in accordance with manufacturers' recommendations, to ensure its availability and integrity. All faults (or suspected faults) will be logged in the Incident Management System, and all changes will be logged in the Change Management System. All regular maintenance checks such as PAT testing will also be recorded.

9. INVENTORY

An inventory will be maintained of file servers and communications equipment and recorded in the current Asset Management System, which will be checked regularly to ensure that the College's assets are accounted for.

10. DISPOSAL OF EQUIPMENT

All items of equipment containing storage media will have any software or sensitive data irretrievably removed before disposal or will be processed by a company that is accredited by ICER (Industry Council for Electronic Equipment Recycling) to recycle IT equipment - providing certification of destruction of data. This shall be in accordance with the Disposal of IT Equipment Policy.

11. POLICY REVIEW

This policy will be reviewed whenever changes affect it or within three years, whichever is the earlier.