Policy Number	FEIT 007
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

Website Filtering Policy

Estates Services & IT

1. PURPOSE

This policy sets out Edinburgh College's approach to internet filtering.

2. SCOPE

This policy applies to all communications between the College's networks and the internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols.

Server-to-server communications, such as email, traffic, backups, automated data transfers or database communications are excluded from this policy.

3. RELATIONSHIP WITH EXISTING POLICIES

This policy forms part of the Information Security Management Framework. It should be read in conjunction with the Information Security Policy.

4. POLICY STATEMENT

The College will make use of internet filtering as part of its approach to managing risks and issues of internet usage.

5. POLICY

This policy enables the College to comply with the following:

- The IT Facilities Acceptable Use Policy
- The College's legal obligations (for instance, the Data Protection Act 2018, General Data Protection Regulation 2016, Copyright Act 1988, Computer Misuse Act 1990, Protection of Children Act 1978, Sexual Offences Act 2003, Criminal Justice and Immigration Act 2008, Counter Terrorism and Security Act 2015).

- Issues of due care towards staff, students and other users of College IT facilities (by making sure, for example, that they are not inadvertently exposed to pornography or offensive material).
- To mitigate information and IT security risks posed by computer viruses, malicious software (malware), spam email, phishing, computer hacking and use of illegal file-sharing by preventing access to sites associated with these risks.

The College blocks access to the following categories of website content:

- Gambling
- Marijuana
- Nudity and Risqué
- Other Adult Materials
- Pornography
- Sports Hunting and War Games
- Weapons (Sales)
- Peer-to-peer File Sharing
- Child Abuse
- Discrimination
- Explicit Violence
- Extremist Groups
- Hacking
- Illegal or Unethical
- Plagiarism
- Proxy Avoidance
- Malicious Websites
- Phishing
- Spam URLs

Maintaining freedom of access to the internet is acknowledged as being of operational importance to the College.

Internet filtering log data will be managed in accordance with the College's IT protocols. General trending and activity reports will be maintained as part of monitoring the effectiveness of this policy.

The IT Services team may block a site(s) or protocols temporarily to protect the College IT facilities and its users from cyber threats such as computer viruses, malicious software (malware), spam email, phishing, computer hacking, Denial of Service (DoS) and use of illegal file-sharing. Sites blocked temporarily will be reviewed and considered for permanent blocking by the Vice Principal Corporate Development.

6. RESPONSIBILITIES

The Vice Principal Corporate Development is responsible for review of this policy.

Heads of departments/faculties will be responsible for approving or rejecting requests for filtering to be applied to or removed from a category of material. Appeals against the decision of the heads will be referred to the Vice Principal Corporate Development or Chief Operating Officer.

The Information Governance Group is responsible for ensuring that a summary of internet filtering categories is published and maintained on the staff intranet.

The Vice Principal Corporate Development is responsible for ensuring that appropriate processes and procedures are established to support this policy.

The IT team should provide support to the Head of Communications, Policy and Research as and when required.

7. POLICY REVIEW

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