Policy Number	FEIT 001
Level	3
Issue	2
Issue date	7 June 2018
Review Date	7 June 2021
Author	Gordon Hope
SMG approval	7 June 2018

Edinburgh College

For the future you want

IT FACILITIES ACCEPTABLE USE POLICY

Estates Services & IT

TABLE OF CONTENTS

1. INTRODUCTION

This is the Edinburgh College IT Facilities Acceptable Use Policy. It sets out the conditions of use, which apply to anyone using any Edinburgh College IT and communications systems, or any other information system that users have permission to access because of their relationship with the College. They apply to regulations for using the systems at any College facility that users may visit.

2. PURPOSE

The College's IT and communications facilities are provided to support College education, and business and community engagement. This policy sets out the conditions of acceptable use that need to be followed in order to:

- Maintain the safe and effective use of systems that we all rely upon to communicate and work effectively on College business;
- Safeguard members of the College community and act in accordance with College values;
- Protect the confidentiality, integrity and availability of the College's IT and communications facilities, information and records;
- Meet our legal and regulatory obligations, including the conditions of use set out by JANET for all users of its electronic networks and communications facilities.

Any user who breaches the conditions of use set out in this policy may be in violation of College regulation and/or criminal or civil law, and will therefore be liable to disciplinary action.

3. SCOPE

This policy applies to:

- Anyone using the IT facilities (hardware, software, data, network access, third party services online services or IT credentials) provided or arranged by Edinburgh College.

- Use of systems, devices and services, including social media, owned by others, access to which has been provided by the College or are otherwise used for College activities. In such cases, the regulations of both bodies apply. In the event of a conflict of the regulations, the more restrictive takes precedence.

- Use of personally owned devices and user service accounts to access College IT accounts, information and communications systems or to process and store College information.

3.1 Expected use
The College provides IT facilities to its users to use in support of their job roles or in connection with their course of study. Reasonable personal use is permitted, but if it is considered by Edinburgh College that excessive, inappropriate or wasteful use is being made of any of the College computer networks for personal use, disciplinary action may be taken against users.

Use of these IT facilities for non-institutional commercial purposes, or for personal gain, requires the explicit approval of the chief operating officer. Such use may be subject to charge.

Certain licenses can be used only for academic purposes and where applicable in line with the College's code of conduct.

3.2 Unauthorised use
Users must not use the College's IT facilities for the creation, storage, display or transmission of any of the following:

- Material which is offensive, obscene, indecent or excessively violent;
- Propagation of any virus, worm, trojan horse or other disruptive programme code;
- Online gambling;
- Material which is designed or likely to cause annoyance or inconvenience;
- Material which discriminates or encourages discrimination on the grounds of, for example: disability, ethnic origin, gender, marital status, sexual orientation, religion or age;
- Material which could constitute harassment or bullying;
- Material which breaches the JANET Acceptable Use Policy;
- The transmission of unsolicited bulk email (spam).

In the online environment, as in all other aspects of College life, all members of the College community need to treat others with dignity and respect, as they themselves should expect to be treated, at all times, in accordance with College values. These apply online and on social networking platforms, such as Facebook and Twitter.

Users must not:

- Attempt to circumvent any IT security controls;
- Carelessly enable the transmission of malware into the network;
- Install software or reconfigure College systems without approval.

Users must not do anything to jeopardise the integrity of the IT infrastructure by, for example, doing any of the following:

- Damaging, reconfiguring or moving equipment;
- Loading software on Edinburgh College's equipment other than in approved circumstances;
- Reconfiguring or connecting equipment to the network other than by approved methods;
- Setting up servers or services on the network, unless approved by the academic head of function for teaching purposes, using a sub-network that is approved by the IT Department and is securely isolated from College systems and the internet;
- Deliberately or recklessly introducing malware;
- Attempting to disrupt or circumvent IT security measures.

Staff are required to purchase and dispose of College IT and communications equipment, software, and devices in accordance with College financial regulations, procurement and IT policies.

4. OBJECTIVES AND CONDITIONS OF USE

The objectives of this policy are to maintain safe and reliable IT and communications for the College community. To this end, all users must comply with the following conditions of use.

4.1 Legal governance

When using IT, users remain subject to the same laws and regulations as in the physical world. It is expected that users' conduct is lawful. Furthermore, ignorance of the law is not considered to be an adequate defence for unlawful conduct.

When accessing services from another jurisdiction, users must abide by all relevant local laws, as well as those applicable to the location of the service.

Users must abide by the regulations applicable to any other organisation whose services they access such as Janet, Eduserv and Jisc Collections.

When using services via Eduroam, users are subject to both the regulations of Edinburgh College and the institution where users are accessing services.

Some software licenses procured by Edinburgh College will set out obligations for the user – these should be adhered to, and users are deemed to have accepted the acknowledgment of third party rights.

Breach of any applicable law or third party regulation will be regarded as a breach of this policy.

4.2 Authority

This policy is issued under the authority of the chief operating officer who is also responsible for its interpretation and enforcement, and who may also delegate such authority to other people.

Users must not use the IT facilities without the permission of the head of Estates and IT Services.

Users must comply with any reasonable written or verbal instruction issued by people with delegated authority in support of this policy. If users feel that any such instructions are unreasonable or are not in support of these regulations, users may appeal to the chief operating officer within Edinburgh College or make a complaint to the College complaints handling coordinator, using the procedure published here.

4.3 Identity

Users must take all reasonable precautions to safeguard any IT credentials (for example, a username and password, smart card or other identity hardware) issued to them.

To this end, users must:

- Not allow anyone else to use their IT credentials. Nobody has the authority to ask a user for his or her passwords and users must not disclose them to anyone;
- Not attempt to obtain or use anyone else's credentials;

- Not impersonate someone else or otherwise disguise user identity when using the IT facilities;
- Use Edinburgh College email addresses for all College business emails.
- Relinquish IT facilities when their employment or period of study with the College ends. The chief operating officer may authorise continued access where this is demonstrably in the interests of the College.

When employees leave, the Human Resources department is responsible for notifying IT services promptly to rescind IT access rights.

Managers and employees are also responsible for ensuring that all information needed by the College is transferred to the manager and that devices issued to users are returned to IT Department.

When students leave, the academic head of function or curriculum manager is responsible for notifying IT Services promptly to rescind IT access rights.

When external visitors, contractors or other people with user privileges who are not staff or students leave, their managers are responsible for notifying IT Services promptly to rescind IT access rights.

Users must take reasonable steps to secure any issued login credentials, smart cards or other similar authentication systems and must not allow anyone else to use their credentials.

- Always choose a strong password;
- Do not communicate your password to a third party;
- Do not leave workstations unlocked when not in attendance;
- Contact the IT service desk immediately if you believe your credentials have been compromised.

4.4 Privileged accounts

Administrator accounts with highly privileged access to systems and data are particularly attractive to attackers. These accounts should not be used for high risk activities such as accessing external email or browsing the internet. Administrators must have a standard user account for normal use with a different password.

4.5 Use of information

All members of the College need to follow the relevant College policies and procedures for data that they create and manage for College work.

If users handle personal, confidential or sensitive information, they are responsible for taking all reasonable steps to safeguard it.

To this end users must not:

- Copy or download confidential information from College systems without authorisation by the relevant officers. Where such authorisation has been received, only secure encrypted methods provided by the College may be used to transmit and store confidential information;

- Infringe copyright, or break the terms of licenses for software or other material;

- Attempt to access, delete, modify or disclose information belonging to other people without their permission, or explicit approval from the chief operating officer;

- Not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. The College reserves the right to block or monitor access to such material.

The College has procedures to approve and manage activities involving such material for valid purposes, where legal, with the appropriate ethical approval.

There will be an exemption covering authorised IT staff involved in the preservation of evidence for the purposes of investigating breaches of the regulations or the law.

4.6 Monitoring

The College reserves the right to monitor use of all of its IT systems to:

- Enforce College policies and detect or investigate any infringements;
- Detect and prevent the propagation of malware or other malicious software;
- Detect and prevent the propagation of spam or other junk email;
- Ensure the effective operation of the college's IT facilities.

Edinburgh College will comply with lawful requests for information from government and law enforcement agencies.

Users must not attempt to monitor the use of the IT facilities without explicit, specific and documented authority from the chief operating officer.

Account lock-out should be enabled for all password systems where these controls are available. If using lockout, ten login attempts should be allowed before the account is frozen.

Network, system and application event monitoring should be used whenever it is available to detect and alert on malicious or abnormal behaviour. This will include automated attempts to guess or brute-force account passwords.

4.7 Infringement

The head of Corporate Development will set up management processes to monitor compliance with this policy and will report to the chief operating officer, Information Management Group, and Risk Assurance Group any breaches of this policy which present information security risks and issues, and agree actions to address these.

The terms of this policy must be observed at all times. Any failure to comply with the terms of this policy may lead to disciplinary action being taken against the user in accordance with the College disciplinary policy and/or legal proceedings.

The type of disciplinary action taken will be dependent on the seriousness of the issue. Factors that will be taken into account include:

- Disruption to the network;
- Creation of a hostile working environment;
- Damage to the college's reputation;
- Breaches of confidentiality, security and the law.

The College reserves the right to:

- Withdraw a user's access to any IT system, including internet services;
- Remove or substitute the hardware or software used at any time and for any reason;

- Pass information to the relevant statutory authorities.

The above list of sanctions is not exhaustive and may be altered or augmented by the College depending on the nature of the incident.

5. LINES OF RESPONSIBILITY

5.1 All users

All users who are given access to College IT and communications facilities are responsible for complying with this policy.

5.2 The Chief Operating Officer

The chief operating officer has senior management accountability for IT services and governance, reporting to the Principal and Chief Executive and the Audit and Risk Assurance Committee on relevant risks and issues.

5.3 Head of Estates and IT Services

The head of Estates and IT Services is responsible for the management and delivery of centrally managed IT systems, for reporting, investigating and taking appropriate action to address breaches of this policy. The head of Corporate Development will liaise with staff responsible for investigating disciplinary incidents involving staff and students and with the other designated officers accordingly to manage information security risks and issues arising from the use of College IT and communications facilities.

5.4 Heads of functions

Heads of functions are responsible for ensuring that all staff responsible for locally managed IT services and information systems maintain appropriate controls to manage their devolved responsibilities for compliance with this policy.

5.5 Head of Procurement

The head of Procurement is responsible for the procurement of all College IT and communications equipment and devices for College business.

6. IMPLEMENTATION

The chief operating officer is responsible for ensuring the effective implementation of this policy and its associated policies and procedures, delegating authority as appropriate to the senior managers set out in paragraph five above. The chief operating officer will ensure that implementation of this policy is supported by

effective procedures, guidance and appropriate generic and role-based communications, training and awareness-raising measures, applicable to all users.

All users are responsible for:

- Taking all reasonable steps to ensure compliance with the conditions of this policy.
- Reporting to the IT service desk any violation of this policy or anything that concerns the fitness of a file or a program on the network.

7. RELATED POLICIES, PROCEDRES AND FURTHER REFERENCE

This policy should also be read in conjunction with the College's disciplinary policies and procedures.

The College's Information Security Policy Framework and associated policies, procedures and guidance which are published on the College website.

The College's Data Protection Policy Statement.

These policies and procedures are reviewed and updated as necessary to maintain an effective Information Security Management System to meet the College's business needs and legal obligations.

7.1 Legal requirements and external standards

Use of IT and communications is subject to UK and Scottish law and other relevant law in all jurisdictions in which the College operates.

All current UK Legislation is published at http://www.legislation.gov.uk/.

All use of College IT and communications facilities is also subject to:

- JANET Acceptable Use Policy https://community.ja.net/library/acceptable-use-policy

- Eduserv: Conditions of use of software and online resources made available under Eduserv.

Data Protection Act 1998	Malicious Communications Act 1988
Computer misuse Act 1990	Copyrights, designs, patents Act 1988
Trade Marks Act 1994	Freedom of Information Act (Scotland) 2002
Sex Discrimination Act 1986	Race Relations Act 1976, 1999
Defamation Action 1996	General Data Protection Regulation (GDPR) 2018

This policy is based on the Universities and Colleges Information Systems Association (UCISA) Model regulations for the use of institutional IT facilities and systems.

8. DEFINITIONS

IT and communications facilities	Information technology, networks, hardware and software systems, servers, user accounts, copying and printing services and equipment, telecommunications, phone, fax, email, messaging, online communications systems and services, whether desktop or mobile, whether provided directly by the College of via third party suppliers.
Information	The definition of information includes, but is not confined to, paper and electronic documents and records, email, voicemail, still and moving images and sound recordings, the spoken word, data stored on computers or tapes, transmitted across networks, printed out or written on paper, carried on portable devices, sent by post, courier or fax, posted onto intranet or internet sites, stored or transmitted using cloud computing services or communicated by social media.
User	Any person or organisation that is given access to IT and communications facilities provided or arranged by the College.
Janet	The computer network serving all UK higher and further education institutions and research councils.

Eduserv	A not-for-profit organisation which negotiates affordable licence agreements for software and online resources for universities and colleges in the UK and Ireland.

9. FURTHER HELP AND ADVICE

For further information and advice about this policy contact:
Email: gordonhope@edinburghcollege.ac.uk
Telephone: 0131 297 8112

10. POLICY VERSION AND HISTORY

Version No	Date of Approval	Approving Authority	Brief Description of Amendment
V14.3	9 April 2018	College Executive	First draft of policy.
V14.4	7 June 2018	Senior Management Group	Final Approval by SMG

11. ADDENDUM – PASSWORD GUIDANCE

11.1 IT Systems password guidelines

1. Factory-set default passwords must not be left unchanged on any system or software before deployment.

2. All users should use a minimum of fourteen (14) characters.

3. Always use unique passwords for your work accounts.

4. Never share your passwords with anyone.

5. Users should make their password difficult to guess. For example, three well-chosen words can be memorable but not easy to guess.

6 Users must change their password on the indication or suspicion of possible compromise.

7. Users should not use the same password when prompted to change or on the indication or suspicion of possible compromise.

8. Use a 'password manager' on your smartphone. These can easily create and maintain long, complex, unique passwords for every service that you use.

11.2 Forgotten passwords

Passwords can be reset at any time by answering three security questions at: https://password.edinburghcollege.ac.uk

Security questions should be completed at:
https://passwordreg.edinburghcollege.ac.uk

If assistance is required from the IT department, User identity will need to be confirmed and validated before the password can be reset.