

TITLE		REF	VERSION
IT Services Acceptable Use Policy		IT004	6
APPROVAL BODY:		DATE	REVIEW DATE
GET		29 September 2024	29 September 2026
LEAD PERSON		Group Director of Institutional Effectiveness	
EQIA DATE	20 September 2024	DPIA DATE	20 September 2024

## IT SERVICES ACCEPTABLE USE POLICY

### Policy Statement

Activate Learning is committed to protecting its commercial interests by ensuring that its information and information processing systems are used in an appropriate manner.

IT services are provided by the College for academic and business purposes in support of the College aims and interests. IT services are made available to a wide range of users on a conditional basis. All users must comply with the Acceptable Use Policy (AUP), which additionally incorporates the JANET Acceptable Use Policy.

Acceptable use of College IT services is lawful, reasonable and raises no unnecessary risks or security threats for the College. Unacceptable use contrary to this and associated IT policies and procedures will be subject to disciplinary procedures as deemed appropriate by the HR department or student's programme area.

This policy applies to all users of College IT services including students, teachers, business support staff, researchers, academics and partners and applies to all IT services offered, regardless of whether a device is owned by an individual or by Activate Learning.

This policy governs the use of all IT services managed by Activate Learning, including any affiliated services provided under contract within Activate Learning-owned premises or accommodation areas. It covers the use of hardware, software, network storage, data, resources, and connections both within and beyond the Activate Learning network.

The policy applies to IT Services and to all services offered via the College Digital Education Services team.

The aims of this policy are:

- To promote the professional, ethical, lawful and productive use of College IT services.
- To define and prohibit unacceptable use of College IT services.
- To educate users about their responsibilities
- To confirm that misuse of the College IT services is a disciplinary offence.

### Purpose

The purpose of this policy is to ensure that IT Services are safe, free from any unnecessary risks to the individual and to ensure the College is not exposed to any security threats with may compromise the business.

### Scope

This policy applies to the use of all IT services administered by Activate Learning, including services provided under contract for Activate Learning. This policy addresses the use of hardware, software, network storage, data, Artificial Intelligence (AI) resources and tools, and resources and connections beyond the Activate Learning network.

## Responsibilities

### Users of Activate Learning's IT Services

This includes, but is not limited to, students, teachers, business support staff, researchers, academics, partners and contractors.

### Third Parties

Third parties are expected to adhere to this policy to the same extent as all 'users' mentioned above. They will act responsibly and in full compliance with this policy. Ensuring that third parties are aware of their obligation to adhere to this policy is the responsibility of the College representative they are engaged to work with/for.

The Group Director of Institutional Effectiveness is responsible for the development, monitoring and review of all IT Services policies, ensuring they are cascaded to all relevant management and staff.

## Principles of the Policy

- Acceptable use of College IT services is lawful, reasonable and raises no unnecessary risks or security threats to Activate Learning.
- IT Services are provided by the College for academic and business purposes to support a range of uses that meet Activate Learning's aims and interests.
- Personal use is not offered as a right and must never interfere with College work. It should be incidental and modest and cause the College no risk or unnecessary expense.
- Internet access and related services are provided to the College by JANET (the Joint Academic Network). Users must comply fully with JANET's Acceptable Use Policy when connecting beyond Activate Learning.
- Acceptable use of AI resources and tools is safe, ethical, and raises no unnecessary risks or security threats to Activate Learning.

## Behaviour

### Acceptable Use

- Registered users are encouraged to use College IT services to further the goals and objectives of their work, study and research.
- 'Personal use' of College IT services is permitted but only on a conditional basis providing it does not cause unwarranted expense, risk or liability, or reputational damage to the College, or otherwise impact upon the delivery of services to others through its scale or nature.
- Users should be aware that they are subject to any regulations applicable at a remote site when accessing College IT services, or to any regulations governing the use of a specific application or service.

### Unacceptable Use

- Unacceptable use includes, but is not limited to, the following activities (other than for properly supervised and lawful research purposes) some of which may be unlawful in certain circumstances:
- Creating, transmitting, storing or displaying offensive, indecent or obscene material.
- Creating, transmitting, storing or displaying material that deliberately or unlawfully discriminates, or encourages deliberate and unlawful discrimination, on the grounds of race, ethnicity, gender, sexual orientation, marital status, age, disability or political or religious beliefs.
- Creating or transmitting defamatory material.
- Obtaining, transmitting or storing material where this would breach the intellectual property rights of another party. This includes downloading and sharing music, video and image files without proper

authority.

- Creating or transmitting material with the intent to defraud.
- Commercial uses unrelated to the interests of Activate Learning.
- Use of College email system that is likely to cause annoyance or inconvenience, for example, sending unsolicited email chain letters.
- Deliberate activities with any of the following characteristics:
  - Wasting staff effort or IT services resources
  - Corrupting or destroying another user's data or violating their privacy
  - Using IT services in a way that denies access to other users
  - Deliberately introducing, executing or transmitting malware
  - Deliberately disabling or compromising any College IT security systems
  - Physical or other purposeful damage to IT services and equipment
- Negligent use of the College network services, for example, failure to follow explicit instructions from IT services

All users of the College IT and Digital Education services must be aware that:

- They are expected to respect copyright and trademarks at all times.
- All use of the College network is monitored, logged, and audited including all internet access. Users can be monitored remotely without prior notice or knowledge of the event.
- Data stored on the College network servers is not private and neither can it be considered 100% secure. All possible precautions are taken to prevent loss of data through malicious or accidental actions.
- Users are responsible for their username and whatever their username may be used for, for example, if a user leaves a computer logged on and unattended, they are responsible for any actions taken under their login.
- Users must not in any circumstances allow other students or staff members to use their login credentials.
- Users must be aware that external agencies, for example the police, may be involved where use of the College IT services is considered to be a criminal offence.
- Any accidental access to inappropriate material online should be reported to IT services immediately.
- Any deliberate access to inappropriate material will lead to disciplinary proceedings in line with HR's behaviour policies or student behaviour policy and may involve external agencies, for example the police.
- A periodic check will be made on the College network to ensure that no illicit material is taking up valuable storage space. All such material will be removed without warning.
- All users are expected to adhere to GDPR guidelines as directed by the Data Protection Officer (DPO). In the event of a safeguarding issue, safeguarding of students and staff remains our priority. Failure to abide by this policy will result in loss of access and further disciplinary action may be taken by HR.

## Ownership and Asset Management

- All IT services provided by the College are considered an Activate Learning asset, whether they are directly owned by the College or are leased from a third party.
- All College assets are tagged and inspected regularly by IT services.
- All College assets must be returned to Activate Learning upon request, or when a user's employment, or study programme ends or is terminated.
- Under no circumstances should a user be permitted to retain any College assets once their relationship with the organisation has ended.

## Breach of the Policy

All breaches of this policy will be subject to an initial investigation by IT services and referred to the Group Director of Institutional Effectiveness where necessary. Many of the activities discussed in this policy have the potential to also be a breach of criminal law. Activate Learning will co-operate in a Police enquiry and will report any matter which appears to constitute a criminal offence.

Serious or persistent breaches may constitute gross misconduct and result in dismissal or withdrawal from the programme of study.

**Further Information about this Policy is available within the “Acceptable Use Procedures”.**

