LIVERPOOL
HOPE
UNIVERSITY
Est. 1844

IT Services

IT

Acceptable Use Policy

Document Control

Responsibility for Policy:	Chief Information Officer
Approved by and date:	USET May 2023
Frequency of Review:	Annual
Next Review date:	April 2024
Related Policies:	None
Minor Revisions:	Change to eligible users, add reference to E-mail Policy and formalise when accounts can be accessed for avoidance of breaches purposes

1. Purpose

The Acceptable Use policy ensures that the benefits of the University's Information Technology resources are maximised and that any potential liabilities are minimised.

This policy makes all users of the University's Information Technology facilities aware of their obligations to use the resources in a responsible, professional, ethical and lawful manner. For the purposes of this policy, Information Technology facilities include:-

- the wired and wireless networks
- the Remote Desktop facility
- University desktops and laptops
- University phones including mobile devices
- printers
- provided software including Student Record Management, Moodle, Internet
- University data
- Social networks including, but not limited to, Facebook, Twitter, WhatsApp, LinkedIn, YouTube, Instagram, Pinterest, Google+ and Tumblr.

The provisions of this policy also apply to non-University owned equipment e.g. personal desktops / laptops, mobile devices when connected to the University networks.

Any staff member or student who is found to have breached this policy will be subject to the University's disciplinary policies.

2. Eligible Users

All current staff and registered / pending students are eligible to use the University's Information Technology facilities. The following groups are **NOT** permitted to use the facilities:-

- Former members of staff unless access approval has been granted by the Director of Personnel for a fixed period of time
- Former students
- Members of the general public

3. Requirements of the Policy

All eligible users must abide by the following regulations:-

- Compliance with all University policies including, but not restricted to,:
  - Information Security Policy
  - Communications Policy
  - Data Protection Policy
  - Portable Data Device Security Policy
  - Wireless Service Policy
  - E-mail Policy
- Compliance with all applicable laws and regulations relating to the use of Information Technology equipment. This includes, but is not restricted to:
  - Computer Misuse Act (1990) which makes activities such as hacking or the deliberate introduction of viruses a criminal offence
  - Criminal Justice Act 1994 amendment to the Obscene Publications Act under which it is a criminal offence to create, store, download or transmit obscene material
  - Data Protection Act 2018
  - Regulation (EU) 2016/679 (General Data Protection Regulation)
  - Respecting the copyright of all materials and software made available by the University or third parties for authorised use
  - The regulations set out by JISC, the electronic communications network and associated electronic communications networking services and facilities which supports the requirements of the UK education and research communities.
- Utilise the facilities for academic and / or University administrative work except for limited, non-commercial personal use
- Treat as confidential any information and software which may become available to them inadvertently. Such information will not be copied, retained, modified or distributed.

- Make no attempt to evade the security mechanisms or deliberately eavesdrop

- Pay any charges which are incurred for the use of the facilities

- Accept that the University may monitor and investigate the use of the resources either for systems maintenance or to ensure that University regulation and all applicable laws are being adhered to.

- Subject to the approval of the Legal Services Governance & Risk Senior Officer, accept that the University may access an individual's University network or e-mail account to prevent legal or regulatory breaches including but not limited to data or security breaches, issues under the Prevent legislation

- Where another network is being accessed via the Liverpool Hope University network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of Liverpool Hope University's network;

4. Unacceptable Use

Users of the I.T. facilities may not:-

- create or transmit any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;

- create or transmit any material of a sexist, racist, libellous or of a terrorist nature or which would breach the University's duty to have due regard to the need to prevent people from being drawn into terrorism or the promotion of hate or violence in any form.

- transmit unsolicited, commercial or advertising material to other users.

- use or produce materials to attempt to gain unauthorised access to University I T facilities including scanning activities;

- use or produce material which attempt to facilitate unauthorised changes or malfunctions to the University I T Services

- create or transmit material which is designed or likely to cause annoyance, inconvenience or needless anxiety;

- create or transmit defamatory material;

- transmit material or use software which infringes the copyright of another person or third party;

- download, copy, store or supply copyright materials including software and retrieved data without the permission of the Copyright holder or under the terms of the license held by the University;

- create or transmit material which is likely to bring the University into disrepute

- communicate via Social Media material which:

    - brings the University into disrepute for example by making defamatory comments about individuals, other organisations or the University;
    - contains images that are inappropriate, links to inappropriate content or inappropriate language;
    - breaches confidentiality for example by revealing confidential information owned by the University relating to its activities or the personal data of any individual who has not given written informed consent for their data to be published;
    - breaches copyright for example by using someone else's content without their permission or failing to reference their work appropriately;
    - may be considered discriminatory against, bullying or harassment of any individual. This would include but is not limited to making offensive or derogatory comments relating to sex, gender, race, disability, sexual orientation, religion, belief or age; using social media to bully another individual; or posting images that are discriminatory or offensive or linking to such content.
    - breaches the terms of service of the specific social network being used. Each social network has different terms of use and community guidelines, which must be followed.

- engage in deliberate activities with any of the following characteristics:

    - Wasting staff effort or IT resources including time
    - Corrupting or destroying other users' data;
    - Violating the privacy of other users;
    - Disrupting the work of other users;
    - Preventing others from using a workstation when they leave the station

- use IT Resources in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment)

- install any software on University equipment or the University IT network that has not been previously approved by IT Services

- continue to use an item of networked software or hardware after the University has requested that use cease because it is causing disruption to the current functioning of the network or is in breach of approved policies;

- continue to use an item of software or hardware after the JISC Network Operations Centre or its authorised representative has requested that use cease because it is causing disruption to the correct functioning of JISC or is in breach of approved policies

- engage in other misuses of the network or networked resources, such as the introduction of 'viruses'

- engage in any other actions that infringe current legislation.

- allow their account to be used by others or disclose their passwords to others

- use accounts or passwords belonging to others

- engage in software theft or abuse of software licenses

- forge e-mail signatures or use University logos for unauthorised purposes

- initiate and / or forward ‘chain’ or ‘junk’ e-mail

- interfere or attempt to interfere with or destroy systems or software set up on public facilities. This includes the loading or attempting to load unauthorised software on central or departmental managed systems and servers

- attempt to open, move, disconnect or in any other way tamper with or attempt to destroy or damage Information Technology equipment. All faults with equipment should be notified to the appropriate support facility

- change, remove, deface or destroy output not originated by the user

- attempt to connect any items of equipment to I T assets belonging to the University without obtaining prior permission.

- leave a workstation which they have logged into unattended for any length of time. I T Services staff will log out any user who has left a workstation unattended.

5. Monitoring of the Policy

- All data and programs which have been created / owned / stored by the user on or connected to the University I T facilities may, in the instance of suspected wrong doing, be subjected to inspection by the University or by statutory bodies. In the event that the data or programs are encrypted or password protected, the user will be required to provide the decryption key / password.

- As provided by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the University will intercept and monitor electronic communications for the purposes permitted under these Regulations.

- In line with the requirements of the JISC Acceptable Use policy, the University will keep logs of user access and their location in order to notify the user of a reported breach of the JISC regulations.

6. Investigation Process

In the event that a breach of the policy is suspected which may require an investigation of the individual's IT accounts, the following procedures will be followed:

- The individual who suspects that the policy has been breached will contact the Chief Information Officer in writing outlining the issue, the supporting evidence and the scope of investigation required.

- The Chief Information Officer, in conjunction with the Data Protection Officer if appropriate, will assess the request and either notify the individual that it has been denied or authorise the investigation to proceed.

- The results of the investigation, including supporting evidence, will, if appropriate, be passed to the Data Protection Officer for review prior to onward communication to the individual who raised the issue.

7. Liabilities

- Other than any statutory obligation, the University will not be liable for any loss, damage or inconvenience arising directly or indirectly from the use of, or prevention of use of, any I T facility provided or managed by the University

- Whilst the University takes appropriate security measures against unauthorised access to, alteration, disclosure or accidental loss of personal and other data, it cannot and does not give any warranties or undertakings to the user about security, confidentiality or integrity of data, personal or other.

8. Policy Review

This policy will be reviewed on an annual basis to identify any required revisions.