UNIVERSITY OF ABERDEEN

Conditions for using Information Technology Facilities

1 Purpose

The purpose of this policy is to ensure that University of Aberdeen digital services and computing facilities are used for their intended purposes and utilised safely, lawfully and equitably. It also serves to protect the confidentiality, integrity and availability of University of Aberdeen digital information and services. For additional guidance, view the summary video and read the accompanying *Guidance Notes*.

2 Scope

These regulations apply to anyone using the IT facilities (hardware, software, data, network access, third party services, online services, or IT credentials) provided or arranged by the University of Aberdeen.

3 Summary

The following is a summary of the main points of the IT Conditions of Use. You are expected to be familiar with the full Conditions for using Information Technology Facilities.

- **Governance**

  Do not break the law, do abide by the University of Aberdeen's regulations and policies, and do observe the regulations of any third parties whose facilities you access.

- **Identity**

  Do not allow anyone else to use your IT credentials, do not disguise your online identity and do not attempt to obtain or use anyone else's credentials.

- **Infrastructure**

  Do not put the institution's IT facilities, business operation or data at risk by introducing malware, interfering with hardware or loading unauthorised software.

- **Information**

  Safeguard personal data, respect other people's information and do not abuse copyright material. Remember that mobile devices may not be a secure way to handle information.

- **Behaviour**

  Do not waste IT resources, interfere with others' legitimate use or behave towards others in a way that would not be acceptable in the physical world.

4 Governance

When using IT, you remain subject to the same laws and regulations as in the physical world.

It is expected that your conduct is lawful. Furthermore, ignorance of the law is not an adequate defence for unlawful conduct.

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

You are bound by University of Aberdeen general regulations when using the IT facilities; these are available in the Policy Zone.

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

When using services via Eduroam, you are subject to both the regulations of the University of Aberdeen and the institution where you are accessing services.

Breach of any applicable law or third-party regulation will be regarded as a breach of these IT regulations and may result in disciplinary procedures.

5 Authority

These regulations are issued under the authority of the Court which has delegated responsibility for their interpretation and enforcement to the Director of Digital and Information Services.

If you have any doubt whether or not you have the authority to use an IT facility you should seek further advice from the IT Service Desk. Attempting to use the IT facilities without the permission of the relevant authority is an offence under the Computer Misuse Act.

You must comply with any reasonable written or verbal instructions issued by people with delegated authority in support of these regulations. If you feel that any such instructions are unreasonable or are not in support of these regulations, you may appeal to the Director of Information Technology.

6 Acceptable Use

IT facilities, including email and login accounts, are provided for use in furtherance of the institution’s mission. Such use might be for learning, teaching, research, knowledge transfer, public outreach, the commercial activities of the institution, the administration necessary to support all the above or other work in connection with your employment by the institution.

Use of these facilities for personal activities, if it does not infringe any of the regulations, is permitted on a limited basis. This is a privilege that may be withdrawn at any point and University of Aberdeen email addresses should not be used to set up personal accounts for services including banking and social media.

Employees using the IT facilities for non-work purposes during working hours are subject to the same management policies as for any other type of non-work activity.

Use of these IT facilities for non-institutional commercial purposes, or for personal gain, requires the explicit approval of the Director of Digital and Information Services.

Use of certain licences is only permitted for academic use and where applicable to the code of conduct published by the Combined Higher Education Software Team (CHEST). See the accompanying *Guidance Notes* for further details.

A University of Aberdeen owned and managed primary device must be used by staff for regular home, hybrid, remote, and on campus working.

7 Identity

Ensure that usernames and passwords are kept secure and not shared with, or disclosed to, any individual.

Nobody has the authority to ask you for your password and you must not disclose it to anyone. You must not allow anyone else to use your IT credentials.

You must not attempt to obtain or use anyone else's credentials.

You must not impersonate someone else or otherwise disguise your identity when using the IT facilities.

8 Infrastructure

You must not do anything to jeopardise the integrity of University Digital services by, for example, doing any of the following:

- Damaging, reconfiguring or moving equipment.
- Loading software on University of Aberdeen 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.
- Deliberately introducing malware.
- Attempting to disrupt or circumvent IT security measures.

9 Information

If you handle personal, confidential or sensitive information, you must take all reasonable steps to safeguard it and must observe the University of Aberdeen's Data Protection and Information Security policies and guidance, available in the Policy Zone, particularly with regard to removable media, mobile and privately owned devices.

You must not infringe copyright or break the terms of licences for software or other material.

You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, threatening or discriminatory. The University of Aberdeen has procedures to approve and manage valid activities involving such material; these are available on the University website and must be observed.

You must abide by University of Aberdeen Code of Practice for Electronic Publishing when using the IT facilities to publish information.

10 Behaviour

The way you behave when using IT service or social media should be no different to how you would behave under other circumstances. The University of Aberdeen policies concerning staff and students also apply to the use of social media. These include human resource policies, codes of conduct, acceptable use of IT and disciplinary procedures.

- Abusive, unlawful, inconsiderate or discriminatory behaviour is unacceptable.
- You must not cause needless offence, concern or annoyance to others.
- Adhere to University of Aberdeen guidelines on social media.
- You must not send spam, malicious email or unsolicited bulk email.
- You must not deliberately or recklessly consume excessive IT resources such as processing power, bandwidth or consumables. Use resources wisely. Do not consume excessive bandwidth by uploading or downloading more material (particularly video) than is necessary. Do not waste paper by printing more than is needed; do not print single sided when double sided would do. Do not waste electricity by leaving equipment needlessly switched on.
- You must not use the IT facilities in a way that interferes with others' valid use of them.
- If you are using shared IT facilities for personal or social purposes, you should vacate them if they are needed by others with work to do. Similarly, do not occupy specialist facilities unnecessarily if someone else needs them.
- When using shared spaces, remember that others have a right work without undue disturbance. Keep noise down (turn phones to silent if you are in a silent study area), do not obstruct passageways and be sensitive to what others around you might find offensive.
- When using IT facilities, failure to report suspicious activities that could potentially compromise or breach the system may be classified as misuse and abuse of the system.

11 Monitoring

The University of Aberdeen reserves the right to intercept email, internet, messaging, collaboration and any other telecommunications systems via all University owned technology and systems, including but not limited to e-mail, computers, smartphones, tablets and internet access where the monitoring and record keeping is necessary to:

- investigate or detect the unauthorised use of the systems.
- establish the existence of facts relevant to the University's business.
- ascertain compliance with regulatory/self-regulatory practices and rules.
- ascertain or demonstrate standards which ought to be achieved by service users using the system.
- protect national security/prevent or detect crime.
- ensure the security or the effective operation of the system.

- monitor communications (but not record keeping) to determine whether communications are relevant to the carrying on of the University's business.

In exercising its right to monitor all communication systems, the University is conscious of its obligations under the UK GDPR and Data Protection Act 2018 and the provisions of The Investigatory Powers (Interception by Businesses etc, for Monitoring and Record-keeping Purposes) Regulations 2018.

Any metadata, telemetry and log information gained will only be used for the stated purpose of monitoring. The University will observe the guidelines laid down by the Information Commissioner's Office in respect of monitoring, including in the workplace. Email, internet access and device access monitoring is carried out to ensure the security of University systems and IT infrastructure. Automated scanning includes, but is not limited to, malware detection, spam analysis and detection, encrypted email detection and large mailblocking. The University will comply with lawful requests for information from government and law enforcement agencies. You must not attempt to monitor the use of the IT facilities without explicit authority from the Director of Digital and Information Services.

12 Compliance

Non-compliance or infringement of this policy may result in action being taken under the University disciplinary procedures. You may also be subject to sanctions including restrictions on access to or use of IT facilities, withdrawal of offending material, fines and recovery of any costs incurred by the University of Aberdeen because of the breach.

If the institution believes that unlawful activity has taken place, it will refer the matter to the police or other enforcement agency.

If the institution believes that a breach of a third party's regulations has taken place, it may report the matter to that organisation.

You must inform the IT Service Desk if you become aware of any infringement of these regulations.

13 Review

This policy is reviewed at least annually to ensure it:

- Remains fit for purpose and accurate.
- Reflects changes in technologies.
- Is aligned to industry best practice.
- Supports continued regulatory, contractual, and legal compliance.

14 References

- IT Conditions of use – Guidance Notes

https://www.abdn.ac.uk/staffnet/documents/policy-zone-information-policies/DIT_cond-IT-guide.pdf

- IT Conditions of Use – Summary video - https://abdn.cloud.panopto.eu/Panopto/Pages/Viewer.aspx?id=a157b7e6-6967-47c6-a544-adb900ad8d92
- Policy Zone
www.abdn.ac.uk/staffnet/governance/policies-and-procedures-134.php
- How to Seek Ethical Approval for your Research
www.abdn.ac.uk/staffnet/research/ethical-approval-2780.php
- Publication Policy
www.abdn.ac.uk/staffnet/documents/policy-zone-information-policies/DIT_e-publishing.pdf
- Disciplinary Procedure for Staff
https://www.abdn.ac.uk/staffnet/documents/policy-zone-employment/Disciplinary_Procedure.pdf
- Disciplinary Procedure for Students
www.abdn.ac.uk/infohub/study/student-discipline.php
- IT Service Desk
www.abdn.ac.uk/staffnet/working-here/it-support

Approval/Review History

Version	Date	Action
1.0	March 2000	Approved
2.0	May 2001	Approved
2.2	December 2005	Approved
2.3	May 2007	Approved
3.0	September 2015	Approved
4.0	Information Governance Committee, 2nd March 2021	Approved
4.1	Information Governance Committee, 6th April 2022	Approved
4.2	Information Governance Committee, 23rd March 2023	Approved
4.3	Information Governance Committee, 1 May 2024	Approved

Policy Metadata

Title	IT Conditions of Use
Author / Creator	Information Security Manager
Owner	Information Security Manager
Date published / approved	23 March 2023
Version	4.3
Reviewed	March 2024
Date of next review	March 2025
Audience	Staff, students and other users of IT Facilities provided by the University of Aberdeen
Related documents	Information Security Policy Data Protection Policy Conditions for using IT Facilities – Guidance Notes Conditions for using IT Facilities – Summary video

	Guidelines for Personal Use Code of Practice for Electronic Publishing Network Connection Policy Disciplinary Procedure (HR)
Subject / Description	This policy covers the use of all IT facilities administered by the University of Aberdeen, including use at the University's property and/or use through any networked links to the University's IT facilities.
Document status	Policy
Equality Impact Assessment	N/A
Theme	IT Security, Information Security Management, Information Management, IT, facilities, computers, peripherals, networks, software, data, email, security, performance, accessibility, data protection, JANET, remote access, access
Keywords	Security, Information Security, IT Security, Acceptable Use