IT and Communications Facilities Acceptable Use Policy

January 2019

Approving authority:	University Executive
Consultation via:	Professional Services Leadership Board, Global Information Governance and Data Protection Group
Approval date:	29 January 2019
Effective date:	29 January 2019
Review period:	Two years from date of approval
Responsible Executive:	Secretary of the University
Responsible Offices:	Information Services and Information Governance
Territorial scope:	University Group, Global

HERIOT-WATT UNIVERSITY
IT AND COMMUNICATIONS FACILITIES
ACCEPTABLE USE POLICY
CONTENTS

1. INTRODUCTION

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

This policy is a constituent part of the Heriot-Watt University Information Security Policy Framework.

2. PURPOSE

The University's IT and communications facilities are provided to support University education, research, and business and community engagement. This policy sets out the conditions of acceptable use that we all need to follow in order to:

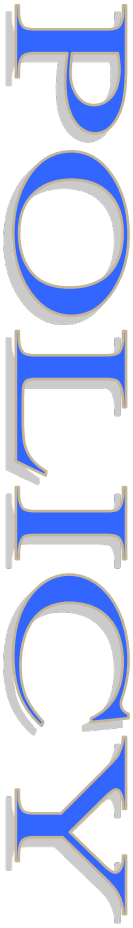
- Maintain the safe and effective use of systems that we all rely upon to communicate and work effectively on University business worldwide;
- Safeguard members of the University community and act in accordance with University values;
- Protect the confidentiality, integrity and availability of the University's 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 University regulations, 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 Heriot-Watt University.
- Use of systems, devices and services, including social media, owned by others, access to which has been provided by the University, or are otherwise used for University activities. In such cases, the



Version 15.1 November 2018. Review of policy approved by UE 22 August 2016
Authors: Ann Jones: based on UCISA model regulations 20140624withaddendum2015
URL: https://www.hw.ac.uk/documents/it-communications-facilities-acceptable-use.pdf

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 University IT accounts, information and communications systems or to process and store University information.

4. OBJECTIVES AND CONDITIONS OF USE

The objectives of this policy are to maintain safe and reliable IT and communications for the University 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 are bound by Heriot-Watt University's information policies when using the IT facilities. These are available here.

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 Heriot-Watt University and the institution where users are accessing services.

Some software licenses procured by Heriot-Watt University will set out obligations for the user – these should be adhered to. If users are using software covered by a Combined Higher Education Software Team (CHEST) agreement, they are deemed to have accepted the Eduserv User Acknowledgment of Third Party Rights. Details of this can be found here.

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

POLICY

4.2 Authority

This policy is issued under the authority of the Secretary of the University 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 Secretary of the University.

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 regulation, users may appeal to the Director of Information Services within Heriot-Watt University or make a complaint to the University Complaints Officer, using the procedure published here.

4.3 Intended Use

The IT facilities are provided for use to support the mission of Heriot-Watt University, for example to support a course of study, research or in connection with a user's employment by the institution.

Use of these facilities for personal activities (provided that it does not infringe this policy, and does not interfere with others' valid use) is permitted, but this is a privilege that may be withdrawn at any point.

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

Certain licenses can be used only for academic purposes and where applicable in line with CHEST licence agreements, as outlined here.

4.4 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 Heriot-Watt University email addresses for all University business emails.

POLICY

- Relinquish IT facilities when their employment or period of study with the University ends. The Director of Information Services or Head of School may authorise continued access where this is demonstrably in the interests of the University.

When employees leave, Human Resources Development is responsible for notifying Information Services promptly to rescind IT access rights.

When students leave, the Academic Registry is responsible for notifying Information Services promptly to rescind IT access rights.

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

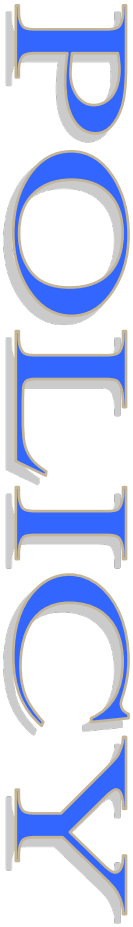
4.6 Infrastructure and use of IT equipment

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 Heriot-Watt University'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 Head of School for teaching purposes, using a sub-network that is securely isolated from University systems and the Internet.
- Deliberately or recklessly introducing malware;
- Attempting to disrupt or circumvent IT security measures.

All University IT and communications equipment, software, and devices must be procured by the relevant responsible services set out in section 5.5 and in accordance with University financial regulations, Procurement and Information Security policies.

When a user of a University issued device leaves the University, managers and employees are responsible for following the Leaver Management Checklist to ensure that all records and information needed by the University are transferred to the manager and that all equipment issued to users, such as mobile phones, laptops, tablets and data storage devices, are returned to Information Services or the relevant School IT Officer. If an employee uses their own device on University business they



need to ensure that any University data is deleted from that device before leaving.

4.7 Use of Information

All members of the University Group need to follow the relevant University information management policies and procedures for data that they create and manage for University 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:

- Comply with Heriot-Watt University's Data Protection and Information Governance policies and guidance, available here. These also apply to data accessed via removable media, mobile and privately owned devices;

- Not copy or download personal data or other confidential information from University systems or disclose it to third parties without authorisation by the relevant officers. Where such authorisation has been received, only secure encrypted methods provided by the University may be used to transmit and store personal data and other confidential information;

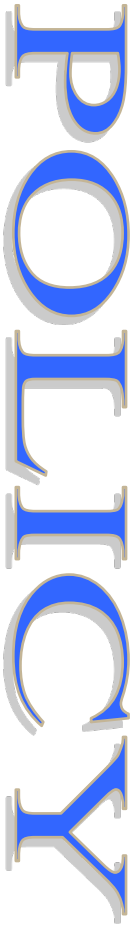
- Not infringe copyright, or break the terms of licenses for software or other material;

- Not attempt to access, delete, modify or disclose information belonging to other people without their permission, or explicit approval from the Secretary of the University;

- Not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. The University reserves the right to block or monitor access to such material. The University has a statutory duty, under the Counter Terrorism and Security Act 2015, termed "PREVENT". The purpose of this duty is to aid the process of preventing people being drawn into terrorism. The University has procedures to approve and manage activities involving such material for valid research purposes, where legal, with the appropriate ethical approval. Universities UK has produced guidance on handling sensitive research materials, available here.

  There is also an exemption covering authorised IT staff involved in the preservation of evidence for the purposes of investigating breaches of the regulations or the law;

- Abide by Heriot-Watt University's Intellectual Property Policy when using the IT facilities to publish information:



4.8 Behaviour

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

Users must not cause needless offence, concern or annoyance to others. Employees also need to adhere to Heriot-Watt University's Social Media Policy and guidelines.

Users must:

- Not send spam (unsolicited bulk email);
- Not deliberately or recklessly consume excessive IT resources such as processing power, bandwidth or consumables;
- Not use the IT facilities in a way that interferes with others' valid use of them;

4.9 Monitoring

Heriot-Watt University monitors and records the use of its IT facilities for the purposes of:

- The effective and efficient planning and operation of the IT facilities;
- Detection and prevention of infringement of this policy;
- Investigation of alleged misconduct or information security incidents; undertaken in line with the University Information Security Incident Management Policy and Procedures.

Heriot-Watt University 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 Director of Information Services.

4.10 Infringement

Infringing this policy may result in sanctions under the University's disciplinary procedures for staff, published here, and students here.

Penalties may include withdrawal of services and/or fines, or in the case of major offences or gross misconduct, sanctions up to compulsory withdrawal or dismissal. Offending material will be taken down.

POLICY

Information about infringement may be passed to appropriate law enforcement agencies, and any other organisations whose regulations Users have breached.

Heriot-Watt University reserves the right to recover from users any costs incurred as a result of their infringement.

Users must inform ITHelp@hw.ac.uk if they become aware of any infringement of this policy.

5. LINES OF RESPONSIBILITY

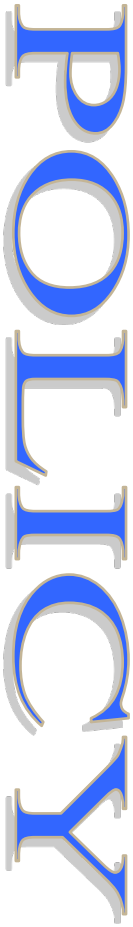
5.1 **All users** who are given access to University IT and communications facilities are responsible for complying with this policy.

5.2 **The Secretary of the University** has senior management accountability for information services and governance, reporting to the University Executive and the Audit and Risk Committee on relevant risks and issues.

5.3 **The Director of Information 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 Director of Information Services will liaise with the Head of Information Governance and Data Protection Officer, staff responsible for investigating disciplinary incidents involving staff and students and with the other designated officers identified in the Information Security Policy Framework to manage information security risks and issues arising from the use of University IT and Communications Facilities.

5.4 **Heads of Schools,** Chief Operating Officers **and Directors of Professional Services** 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 **Information Services**, with support from Procurement Services, is responsible for the procurement of all mobile phones, which must be ordered through the University framework supplier agreement, and all other University IT and communications equipment and devices, except where purchasing authority has been delegated to a School or University Group company by agreement with the Secretary of the University and Information Services.



6. POLICY MONITORING AND EVALUATION

6.1 The Director of Information Services will set up management processes to monitor compliance with this policy and will report to the Head of Information Governance and Data Protection Officer and the Global Information Governance and Data Protection Group any breaches of this policy which present information security risks and issues, and agree actions to address these.

7. IMPLEMENTATION

The Secretary of the University 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 5 above. The Secretary of the University 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.

8. RELATED POLICIES, PROCEDURES AND FURTHER REFERENCE

8.1. This policy should also be read in conjunction with the University's Disciplinary policies and procedures:
For staff, published at https://www.hw.ac.uk/services/human-resources/human-resources-policies.htm

For students: https://www.hw.ac.uk/students/studies/record/discipline.htm

The University's Information Security Policy Framework and associated policies, procedures and guidance which are published in the Information Governance and IT Policies section of the University website here:

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

8.2 Legal Requirements and external standards

Use of IT and communications is subject to U.K. and Scottish law and other relevant law in all jurisdictions in which the University operates.

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

All use of University IT and Communications Facilities is also subject to

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

POLICY

- Eduserv: User Acknowledgement of Third Party Rights Conditions of use of software and online resources made available under Eduserv negotiated Chest Agreements

This policy is based on the Universities and Colleges Information Systems Association (UCISA) Model regulations for the use of institutional IT facilities and systems, March 2014 and subsequent additions. The model regulations and their underpinning guidance are published here: http://www.ucisa.ac.uk/modelregs

9. 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 University or 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 University
Janet	The computer network serving all UK higher and further education institutions and research councils, part of Jisc.
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, part of Jisc.

10. FURTHER HELP AND ADVICE

For further information and advice about this policy contact:
Email: IThelp@hw.ac.uk
Telephone: 0131 451 4045
https://support.hw.ac.uk/

POLICY

11. POLICY VERSION AND HISTORY

Version No	Date of Approval	Approving Authority	Brief Description of Amendment
V15.1 22/11/2018	29/01/2019	University Executive	Update of policy last approved on 11/08/2016. Roles and remit updated and endorsed by GIGDPG for onward approval; territorial scope added to title page. Updated policy on procurement and return of mobile devices to University.

POLICY