UHI | INVERNESS

UHI

# University of the Highlands and Islands Partnership

# Information Security - Acceptable Use Policy

PL/IT/2020/001

| | |
|---|---|
| Procedure Owner | Depute Principal Planning & Student Experience |
| Lead Officer | Depute Principal Planning & Student Experience |
| Review Officer | ICT Services Manager |
| Date first approved by BoM | 20 December 2016 |
| First Review Date | 30 September 2018 |
| Date review approved by BoM | 01 December 2020 |
| Next Review Date | 01/08/2024 |
| Equality impact assessment | |
| Further information (where relevant) | |

| Reviewer | Date | Review Action/Impact |
|---|---|---|
| | | |

## Control

### 1.1 Author and Version Control

| | |
|---|---|
| **Original author:** | Simon Young |
| **Current revision author: (if applicable)** | |

**Version Control**

| Version | Date | Author | Purpose/change | Policy review date |
|---|---|---|---|---|
| 01 | 30/03/16 | Simon Young | Changes for partnership policies | 30/09/2018 |
| 02 | 11/03/19 | Simon Young | Annual Review | 11/03/2020 |
| 03 | 03/10/19 | Simon Young | Removed signature sheet | 11/03/20 |
| 04 | 04/09/2020 | Simon Young | Reviewed and modified from DPA 1998 to DPA 2018 | 04/09/2021 |

## 1.2 Policy Summary

| | |
|---|---|
| **Overview**<br>**Why is the policy required?** | This Acceptable Use Policy is part of the ISO/IEC 27001:2013 policy documentation set and is a requirement to ensure that relevant staff, students and contractors understand their obligations in the use of the university partnership email and Internet facilities. |
| **Purpose**<br>**What will it achieve?** | This policy offers protection and guidance for users and ensures compliance with security good practice and legal requirements. |
| **Scope**<br>**Who does it apply to?** | It applies to all personnel whether staff, students, contractor, or other third party with access to the university partnership's data or information systems. |
| **Consultation/notification**<br>**Highlight plans/dates** | |
| **Implementation and monitoring**<br>**(including costs)** | |
| **Enforcement**<br>**Detail how the policy will be enforced and who will be responsible** | |
| **References**<br>**(highlight any advice received from external organisations)** | |

# SECTION 2

## Introduction

### 2.1 Purpose

This policy is in place to protect the university partnership organisations and employees from illegal or damaging actions that might result from misuse of the university partnership's network. Although specifically aimed at protecting the university partnership's own systems and reputation, it aligns with the Acceptable Use Policy provided by the "JANET" network.

### 2.2 Scope

This policy applies to persons authorised to use the university partnership's network including its own members to whom it provides network access.

This includes, but is not limited to:

- computer equipment;
- software;
- operating systems;
- storage media;
- own equipment (such as home PCs, mobile and smart-phones);
- network accounts providing electronic mail;
- world wide web (www) browsing;
- File copying, e.g., using the file transfer protocol (FTP).

### 2.3 Compliance

This policy applies to all users of the university partnership's systems (viz. all students, staff, contractors and third parties employed by university partnership) and any personal device used on university partnerships premises whether connected to the university partnership or a third party network, and it provides guidance on acceptable standards for using information technology (IT) equipment throughout the partnership.

Indications of non-compliance with the provisions of this policy shall be investigated in accordance with the disciplinary or contractual procedures in place with the university partnership as appropriate.

### 2.4 Terminology

The word "**shall**" is used throughout this document to state where a policy is a mandatory requirement.

The word "**should**" is used throughout this document to state where a policy is a recommended requirement.

For the purposes of this policy the term "**personnel**" includes university partnership staff, contractors, students and third parties who have access to Information Systems.

**"JANET"** (originally a contraction of "Joint Academic NETwork") is the name given both to an electronic communications network and a collection of electronic communications networking services and facilities that support the requirements of the UK education and research community. All further and higher education organisations in the UK are connected to JANET, as are all the Research Councils, across the UK. This network also carries traffic between schools within the UK, although many of the schools' networks maintain their own general Internet connectivity.

# SECTION 3

## Policy

### 3.1 Introduction

The university partnership seeks to promote and facilitate the proper and extensive use of information technology in the interest of learning and research. Whilst the tradition of academic freedom will be fully respected, this also requires responsible and legal use of the technologies and facilities made available to students and staff at the university partnership.

This acceptable use policy is intended to provide a framework for such use of the university partnership's IT resource. It applies to all computing, telecommunication, and networking facilities provided by any department or section of the university partnership.

This acceptable use policy is taken to include the JANET Acceptable Use Policy and the JANET Security Policy published by JANET (UK) and the Eduserv General Terms of Service Members of the university partnership and all other users of the university partnership's facilities are bound by the provisions of these policies in addition to this acceptable use policy. They are also bound by such other policies as published by the university partnership in the IT support section of the university's intranet. It is the responsibility of all users of the university partnership's IT services to read and understand this policy.

### 3.2 Purpose of Use

The university partnership's computer resources are provided primarily to facilitate a person's essential work as an employee or student or other role within the university partnership.

Use for other purposes, such as personal electronic mail or recreational use of the world wide web, is a privilege, which can be withdrawn, not a right. Any such use must not interfere with the user's duties or studies or any other persons use of the computer systems and must not, in any way, bring the university partnership into disrepute. Priority must always be granted to those needing the facilities for academic work.

University partnership e-mail addresses and associated university partnership e-mail systems must be used for all official university partnership business, in order to facilitate audit and institutional record keeping. All staff and students must regularly read their university partnership e-mail.

Commercial work for outside bodies, using centralised managed services, requires the explicit permission from the director of learning and information services; such use, whether or not authorised, may be liable to charge.

### 3.3 Responsibilities

All personnel, as described in Section 2.4 Terminology, shall comply with this policy.

The **information security officer** shall be responsible for ensuring that this policy is disseminated amongst relevant personnel and the principles incorporated into an Information Security Awareness programme.

**Line managers** shall ensure that staff and contractors for whom they have responsibility are properly briefed on this policy.

**Human resources** shall ensure that the principles of this policy are incorporated into induction training for new staff and contractors.

All users must affirm that they have read and agreed to this Acceptable Use Policy.

### 3.4 Review period

This policy shall be reviewed and updated, if appropriate, after a period of twelve months.

### 3.5 Authorisation

In order to use the computing facilities of the university partnership a person must first be registered. Registration of all members of staff and registered students is carried out automatically. Others must apply to the IT service desk (https://www.uhi.ac.uk/en/lis/). Registration to use university partnership services implies, and is conditional upon, acceptance of this acceptable use policy, for which a signature of acceptance may be required on joining the university partnership. The lack of a signature does not exempt an individual from any obligation from this policy.

The registration procedure grants authorisation to use the core IT facilities of the university partnership. Following registration, a username and password will be allocated. Authorisation for other services may be granted automatically dependent on the role performed or requirements of the persons' academic programme, or requested by application to the IT service desk.

All individual allocated usernames, passwords and e-mail addresses are for the exclusive use of the individual to whom they are allocated. Passwords should be changed from the default on the first login and should follow password best practice guidelines. The user is personally responsible and accountable for all activities carried out under their username. The user should make sure they do not leave a workstation or device they are logged into unattended and should ensure they are logged out at the end of their session. Attempts to access or use any username or e-mail address which is not authorised to the user, is prohibited. No one may use, or attempt to use, IT resources allocated to another person, except when explicitly authorised by the provider of those resources.

All users must correctly identify themselves at all times. A user must not masquerade as another, withhold their identity or tamper with audit trails. A user must take all reasonable precautions to protect their resources. In particular, passwords used must adhere to current password policy and practice.

## 3.6 Privacy

It should be noted that IT staff, who have the appropriate privileges, have the ability, which is occasionally required, to access all files, including electronic mail files. It is also occasionally necessary to intercept network traffic. In such circumstances appropriately privileged staff will take all reasonable steps to ensure the privacy of service users. The university partnership fully reserves the right to monitor e-mail, internet access, telephone and any other electronically-mediated communications, whether stored or in transit, in line with its rights under the Regulation of Investigatory Powers Act (2000) www.opsi.gov.uk/acts/acts2000/ukpga_200000023_en_1.

Reasons for such monitoring may include the need to:

- Ensure operational effectiveness of services;
- Prevent a breach of the law, this policy, or other university partnership policy;
- Investigate a suspected breach of this law, this policy, or other university partnership policy;
- Monitor standards.

Access to staff and student files, including e-mail files, will not normally be given to another member of staff unless authorised by a member of the senior management team at each partner, or nominee, who will use their discretion, if appropriate. In such circumstances the head of section, or more senior line manager, or in the case of an HE student, the university dean of students, will be informed, and will normally be consulted prior to action being taken. Such access will normally only be granted in the following circumstances:

- Where a breach of the law or a breach of this or another university partnership policy is suspected;
- When a documented and lawful request from a law enforcement agency such as the police or security services has been received;
- On request from the relevant head of section, where the managers or co-workers of the individual require access to e-mail messages or files, which are records of university partnership activity, and the individual is unable, e.g. through absence, to provide them.

The university partnership sees student privacy as desirable but not as an absolute right, hence students should not expect to hold or pass information, which they would not wish to be seen by members of staff responsible for their academic work. In addition to when a breach of the law or of this policy is suspected, or when a documented and lawful request from law enforcement agency such as the police or security services has been received, IT staff are also authorised to release the contents of student's files, including e-mail files, when required to by any member of staff who has a direct academic work-based reason for requiring such access.

After a student or member of staff leaves the university partnership, files which are left behind on any computer system owned by the university partnership, including servers and including e-mail files, will be considered to be the property of the university partnership, staff should make arrangements to transfer to colleagues any e-mail or other computer-based information held under their personal account, as this will be closed on their departure.

## 3.7 Behaviour

No person shall jeopardise the integrity, performance or reliability of computer equipment, software, data and other stored information. The integrity of the university partnership's computer systems is put at risk if users do not take adequate precautions against malicious software, such as computer virus programs. All users of the university partnership's IT services must ensure that any computer, for which they have responsibility and which is attached to the university partnership's network, is adequately protected against viruses, through the use of up to date anti-virus software (any exceptions to this must be approved by the director of learning and information services), and has the latest tested security patches installed. Reasonable care should also be taken to ensure that resource use does not result in a denial of service to others.

N.B. All university partnership computers connected to the network are updated on a routine basis

Conventional norms of behaviour apply to ICT-based media, just as they would apply to more traditional media. Within the university partnership setting this should also be taken to mean that the tradition of academic freedom will always be respected. The university partnership, as expressed in its Equality and Diversity Charter, is committed to achieving an educational and working environment which complies with the Equality Act 2010.

Distributing material, which is offensive, obscene, abusive or extremist, may be illegal and may also contravene the university partnership's policy on harassment and bullying and the university partnership's policy on social media and may result in disciplinary action.

No user shall interfere or attempt to interfere in any way with information belonging to or material prepared by another user. Similarly, no user shall make unauthorised copies of information belonging to another user. The same conventions of privacy should apply to electronically held information as to that held on traditional material such as paper.

For specific services the university partnership may provide more detailed guidelines, in addition to the policies provided in this acceptable use policy.

Users of services external to the university partnership are expected to abide by any policies, rules and codes of conduct applying to such services. Any breach of such policies, rules and codes of conduct may be regarded as a breach of this acceptable use policy and be dealt with accordingly. The use of university partnership credentials to gain unauthorised access to the facilities of any other organisation is similarly prohibited.

## 3.8 Definitions of Acceptable & Unacceptable Usage

Unacceptable use of the university partnership's computers and network resources may be summarised as:

- the creations, retention or propagation of material that is offensive, obscene, indecent or extremist, except in the course of recognised research or teaching that is permitted under UK and international law; propagation will normally be considered to be a much more serious offence;

- intellectual property rights infringement, including copyright, trademark, patent, design and moral rights, including use internal to the university partnership;
- causing annoyance, inconvenience or needless anxiety to others, as specified in the JANET Acceptable Use Policy;
- defamation (genuine scholarly criticism is permitted);
- unsolicited advertising, often referred to as "spamming";
- sending e-mails that purport to come from an individual other than the person actually sending the message using, e.g., a forged address;
- attempts to break into or damage computer systems or data held thereon;
- actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software;
- attempts to access or actions intended to facilitate access to computers for which the individual is not authorised;
- using the university partnership's network for unauthenticated access;
- unauthorised resale of the university partnership's or JANET services or information;
- excessive IT use during working hours that significantly interferes with a staff member's work, or that of other staff or students.
- the recording audio/visual of others without their permission
- using the university partnership's network to access gambling sites

These restrictions should be taken to mean, for example, that the following activities will normally be considered to be a breach of this policy (potential exceptions should be discussed with IT):

- the downloading, uploading, distribution, or storage of music, video, film, or other material, for which you do not hold a valid licence, or other valid permission from the copyright holder;
- the use of peer-to-peer software and related applications to illegally download and/or share music, video, film, or other material, in contravention of copyright law
- the publication on external websites of unauthorised recordings, e.g. of lectures;
- the distribution or storage by any means of pirated software;
- connecting an unauthorised device to the university partnership network, i.e. one that has not been configured to comply with this policy and any other relevant regulations and guidelines relating to security, IT purchasing policy, and acceptable use. This includes network hubs, switches and wireless access points not approved or managed by IT but excludes halls of residence.
- circumvention of Network Access Control;
- monitoring or interception of network traffic, without permission;
- probing for the security weaknesses of systems by methods such as port-scanning, without permission;

- associating any device to network Access Points, including wireless, for which you are not authorised;
- non-academic activities which generate heavy network traffic, especially those which interfere with others' legitimate use of IT services or which incur financial costs;
- frivolous use of university partnership owned computer laboratories, especially where such activities interfere with others' legitimate use of IT services;
- opening an unsolicited e-mail attachment, especially if not work or study-related;
- the deliberate viewing and/or printing of pornographic images;
- the passing on of electronic chain mail;
- posting of defamatory comments about staff or students on social networking sites;
- the creation of web based content, portraying official university partnership's business without express permission or responsibility;
- the use of the university partnership business mailing lists for non-academic purposes;
- the use of CDs, DVDs, and other storage devices for copying unlicensed copyright software, music, etc.;
- the copying of other people's web site, or other, material without the express permission of the copyright holder;
- plagiarism, i.e. the intentional use of other people's material without attribution.

Other uses may be unacceptable in certain circumstances. The installed machine on each network socket must be a workstation only and not provide any server based services, including, but not limited to, Web, FTP, IRC, Streaming media server, peer to peer facilities, or e-mail services.

It should be noted that individuals may be held responsible for the retention of attachment material that they have received, via e-mail that they have never opened, via e-mail that they have read. Similarly, opening an attachment, received via unsolicited e-mail, especially if clearly unrelated to work or study, which leads to widespread virus infection, may result in disciplinary action being taken.

Acceptable uses may include:

- Personal e-mail and recreational use of internet services, as long as these are in keeping with the framework defined in this policy document and do not interfere with one's duties, studies or the work of others.

However, such use must be regarded as a privilege and not as a right and may be withdrawn if abused or if the user is subject to a disciplinary procedure.

### 3.9 Personal Safety

- Users will not e-mail personal contact information about other people without their consent. Personal contact information includes the address, telephone, work address, etc.

- Student users should promptly disclose to a member of staff or other university partnership employee any message they receive that they feel is inappropriate or that makes them feel uncomfortable.

### 3.10 Inappropriate Language

- Restrictions against inappropriate language apply to public and private e-mail messages; file names, the content of files and material posted on web pages.
- Such inappropriate language includes obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.

### 3.11 E-mail Misuse

- Users will not email information that could cause damage or a danger of disruption.
- Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person.
- Users will not knowingly or recklessly e-mail false or defamatory information about a person or organisation.
- Users will not forward an e-mail that was sent privately without permission of the person who sent the message.
- Users will not e-mail private information about another person.

## SECTION 4

### Legal Constraints

Any software and / or hard copy of data or information which is not generated by the user personally and which may become available through the use of the university partnership's computing and communications resource shall not be copied or used without permission of the university partnership's copyright owner. In particular, it is up to the user to check the terms and conditions of any license for the use of software or information and to abide by them. Software and / or information provided by the university partnership may only be used as part of the user's duties as an employee or student of the university partnership or for educational purposes. The user must abide by all licensing agreements for software entered into by the university partnership with other parties, noting that the right to use any such software outside the university partnership will cease when an individual leaves the institution. Any software on a privately owned computer that has been licensed under a university partnership agreement must then be removed from it, as well as any university partnership owned data, such as documents and spread sheets. When a computer ceases to be owned by the university partnership all data and software must be removed from it.

The user must comply with all relevant legislation and legal precedent including the provisions of the following acts of parliament, or any re-enactment thereof:

- Copyright, design and patents act 1988
  www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm
- Malicious communications act 1988
  www.opsi.gov.uk/acts/acts1988/Ukpga_19880027_en_1.htm

- Computers misuse act 1990
  www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm
- Criminal justice and public order act 1994
  www.opsi.gov.uk/acts/acts1994/Ukpga_19940033_en_1.htm
- Trade marks act 1994
  www.opsi.gov.uk/acts/acts1994/Ukpga_19940026_en_1.htm
- Data protection act 2018

  www.opsi.gov.uk/acts/Ukpga/2018/12/contents/enacted
- Human rights act 1998
  www.opsi.gov.uk/acts/acts1998/Ukpga_19980042_en_1.htm
- Regulation of investigatory powers act 2000
  www.opsi.gov.uk/acts/acts2000/Ukpga_20000023_en_1.htm
- Telecommunications (lawful business practice)(interception of communications)regulations 20000
  www.opsi.gov.uk/acts/si/si2000/ukpga_20002699.htm
- Freedom of information act Scotland 2002
  www.legislation.gov.uk/asp/2002/13/contents
- Communications act 2003
  www.opsi.gov.uk/acts/acts2003/ukpga_20030021_en_1
- Equality Act 2010
  www.legislation.gov.uk/ukpga/2010/15/contents
- Counter Terrorism and Security Act 2015
  www.legislation.gov.uk/ukpga/2015/6/contents

See below for a summary of the main points.

**Copyright, designs and patent act 1988**

This act, together with a number of statutory instruments that have amended and extended it, controls copyright law. It makes it an offence to copy all, or a substantial part, which can be a quite small portion, of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The act also provides for moral rights, whereby authors can sue if their name is not included in work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers material in print and electronic form, and includes words, images, sound and moving images, TV broadcasts and many other media.

**Malicious Communications Act 1988**

Under this Act it is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person. Additionally, under the Telecommunications Act 1984 it is a similar offence to send a telephone message, which is indecent, offensive, or threatening.

**Computer Misuse Act 1990**

This Act makes it an offence:

- to erase or amend data or programs without authority;
- to obtain unauthorised access to a computer;
- to "eavesdrop" on a computer;
- to make unauthorised use of computer time or facilities;
- maliciously to corrupt or erase data or programs;
- to deny access to authorised users.

**Criminal Justice & Public Order Act 1994**

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

**Trade Marks Act 1994**

This Act provides protection for Registered Trade Marks, which can be any symbol (words or images) or even shapes of objects that are associated with a particular set of goods or services. Anyone who uses a Registered Trade Mark without permission can expose themselves to litigation. This can also arise from the use of a Mark that is confusingly similar to an existing Mark.

**Data Protection Act 2018**

UHI has a comprehensive Data Protection Policy

The policy applies to all staff and students of UHI. Any breach of the Data Protection Act 2018 or UHI Data Protection Policy is considered to be an offence and in that event, UHI disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with UHI, and who have access to personal information, will be expected to have read and comply with this policy.

**Human Rights Act 1998**

This act does not set out to deal with any particular mischief or address specifically any discrete subject area within the law. It is a type of higher law, affecting all other laws. In the context of UHI, important human rights to be aware of include:

- the right to a fair trial;
- the right to respect for private and family life, home and correspondence;
- freedom of thought, conscience and religion;
- freedom of expression;
- freedom of assembly;
- prohibition of discrimination;
- the right to education.

These rights are not absolute. UHI, together with all users of its LIS services, is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations which arise from other relevant legislation.

**Regulation of Investigatory Powers Act 2000**

The Act states that it is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic (including telephone) communications to is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.

Monitoring but not recording is also permissible in order to:

- Ascertain whether the communication is business or personal;
- Protect or support help line staff.

UHI reserves the right to monitor e-mail, telephone, and any other communications in line with its rights under this act. The Lawful Business Practice Regulations allow exceptions to the basic principle of non-interception as stated in the RIPA, and allow interception without consent in certain instances.

**Freedom of Information Act 2000**

The Act, intended to increase openness and transparency, obliges public bodies, including Further / Higher Education Institutions, to disclose a wide range of information, both proactively and in response to requests from the public. The types of information that may be have to be found and released are wide-ranging, for example minutes recorded at a board meeting of the institution or documentation relating to important resolutions passed. Retrieval of such a range of information places a considerable burden on an institution subject to such an information request. In addition to setting a new standard of how such bodies disseminate information relating to internal affairs, the Act sets time limits by which the information requested must be made available, and confers clearly stated rights on the public, regarding such information retrieval. UHI has its own Freedom of Information policy.

**Communications Act 2003**

This act makes it illegal to dishonestly obtain electronic communication services, such as email and the World Wide Web.

**Equality Act 2010**

The Act simplifies, strengthens and harmonises the current legislation to provide Britain with a new discrimination law which protects individuals from unfair treatment and promotes a fair and more equal society.

The nine main pieces of legislation that have merged are:

- the Equal Pay Act 1970;
- the Sex Discrimination Act 1975;
- the Race Relations Act 1976;
- the Disability Discrimination Act 1995;
- the Employment Equality (Religion or Belief) Regulations 2003;
- the Employment Equality (Sexual Orientation) Regulations 2003;
- the Employment Equality (Age) Regulations 2006;
- the Equality Act 2006, Part 2;
- the Equality Act (Sexual Orientation) Regulations 2007.

**Counter Terrorism and Security Act 2015**

UHI 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.
You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. UHI reserves the right to block or monitor access to such material.

## SECTION 5

### Discipline

Staff or students who break this acceptable use policy will find themselves subject to the university partnership's disciplinary procedures. Individuals may also be subject to criminal proceedings. The university partnership reserves its right to take legal action against individuals who cause it to become involved in legal proceedings as a result of their violation of licensing agreements and / or other contraventions of this policy.