Ulster University Policy Cover Sheet

Document Title	Acceptable Use of Information Technology Code of Practice 5.2
Custodian	Chief Digital and Information Officer
Approving Committee	Library, Information and Student Administrative Services Committee (LISASC), then Senior Executive Team (SET)
Policy approved date	2018 – 09 – 12
Policy effective from date	2018 – 09 – 12
Policy review date	2019 – 09 – 12

Changes to previous version
Page 2 – “Data Protection Act 1998” changed to “Data Protection Act 2018” and General Data Protection Regulation (GDPR) added Page 3 – Reference to GDPR added and Data Protection Act updated from 1998 to 2018 within user liabilities and responsibilities clause Page 3 - Clause regarding proactive steps to counteract compromised account spamming added

ULSTER UNIVERSITY

Acceptable Use Code of Practice

1. INTRODUCTION AND BACKGROUND

The University furnishes information and communications equipment, networks, systems and services to staff, associates, visitors and students with the express purpose of furthering the University's corporate aims and objectives. The University is committed to:

- Protecting its employees, students, associates, partners, itself and its investment from consequences of illegal and/or damaging use of such equipment and services
- Ensuring the use of such equipment and services is compatible with and appropriate to its corporate aims and objectives

This Acceptable Use Code of Practice provides users of the University's information and communications equipment, networks, systems and services (including telephony) with current detailed information including:

- What is acceptable use
- What is unacceptable use
- Information on current relevant legislation
- Information other relevant related policies and procedures

The University will regularly review this Acceptable Use Code of Practice, and all staff and students are expected to consult with it regularly, and will be notified of any significant alterations.

Further information on ISD policies, standards and guidelines is available at:

http://ulster.ac.uk/isd/about-us/policies

2. RELEVANT LEGISLATION

The University will comply with all legislation and statutory requirements relevant to acceptable use of University information and communications equipment, networks, systems and services including:

- Protection of Children Act 1999;
- The Sexual Offences *(*Northern Ireland*)* Order 2008*;*
- Police and Criminal Evidence Act 1984 ;
- Copyright, Designs & Patents Act 1988 ;

- Computer Misuse Act 1990 ;
- Human Rights Act 1998 ;
- Data Protection Act 2018;
- Communications Act 2003;
- Regulation of Investigatory Powers Act 2000 ;
- Freedom of Information Act 2000 ;
- Employment Act 2008;
- Prevention of Terrorism Act 2005 ;
- Terrorism Act 2006 ;
- Police and Justice Act 2006;
- General Data Protection Regulation (GDPR)

This list is not exhaustive, and shall be subject to change.

3. RELEVANT RELATED POLICIES AND PROCEDURES

Other applicable policies include:

- JANET Acceptable Use Policy;
- Ulster University IT Monitoring Policy;
- Ulster University Core Values, as defined in the Corporate Plan;
- Ulster University Finance Regulations;
- Ulster University ISMS Policy and Scope

This list is not exhaustive, and shall be subject to change.

4. SCOPE

The scope of this Code of Practice is all authorised users of the University's information and communications equipment, networks, systems and services (including telephony), including all University staff, associates, visitors, students, contractors and external service providers. This also includes devices not owned by the University but connected to the University's networks and systems.

5. IMPLEMENTATION

5.1 Acceptable Use

The Ulster University defines Acceptable Use as the use of University information and communications equipment, networks, systems and services in support of the official business of the University. In this context, this includes teaching, learning and

research, along with administrative and business functions, employment related purposes, or any other permitted activity, including:

- Official trade union business conducted in accordance with the University "Facilities & Time-Off Agreement";
- University sponsored training, educational and/or Continuing Professional Development courses
- some limited personal use which does not:
    - Contravene this Code of Practice;
    - Interfere with the performance of staff work duties, research or study;
    - Impair availability or performance of services for other users.

  The University considers such use a privilege and not a right. The University reserves the right to oversee personal use and permit or refuse it.

As always, the University expects conformance to the University's Core Values, including honesty, integrity and respect for others.

Users may become aware of information, which may be of a confidential nature, concerning staff, students or University business. Users must not improperly disclose, store, transport, retain or misuse personal or confidential information (whether expressly identified or not). When uncertain about the status of information Users should in the first instance liaise directly with their Manager, Supervisor or Course Director.

Users should also be aware of liabilities and responsibilities under GDPR and the Data Protection Act 2018, whereby legal liability may exist for disclosure of information to unauthorised sources. Alleged breaches of confidentiality for sensitive information will be investigated and may result in action under the University's disciplinary procedures.

In the case of long-term illness or extraordinary absence, the University reserves the right to access University e-mail and storage for the purpose of business continuity.

In the event that systems monitoring identifies that an email account is compromised and actively spamming, the University reserves the right to take appropriate proactive steps to protect the integrity of the email service for all users and the information held within that mailbox. These actions may include a password change and blocking an account sending email. For security reasons this may be initiated in advance of communication with the user.

Users may also need to access the systems of other organisations and bodies, and should be aware of and comply with particular arrangements and safeguards for that information.

Acceptable use requires that users make themselves aware of the nature and protective marking classification of systems and information they access and be aware of, and comply with, the University Information Assurance policies.

Some further aspects of acceptable use:

- Facilities must be used for the purposes and in the way they were intended to be used. Other use may be allowed as a privilege, not a right;
- Users must adhere to the terms and conditions of all licence agreements relating to facilities and information which they use including software, equipment, services, documentation and other goods.

5.2 Unacceptable Use

This section defines unacceptable use, describing some related aspects.

Some activities which are acceptable in other environments may be unacceptable within the University.

In general, use that falls within the following categories is considered unacceptable:

- Infringement of the law;
- Infringement of the University's Policies;
- Misrepresentation of the individual or the University;

And with regard to personal use:

- Incurs a significant cost to the University;
- Involves storage or transmission of large amounts of data;
- Interferes with official duties, research or study.

5.2.1 Illegal Materials

The viewing of certain materials and images is a criminal offence and one which the University is obliged to report to the Police Service of Northern Ireland and which may also be investigated by other law enforcement agencies. Examples of materials that would fall into this category are:

- Unacceptable images or texts concerning children;
- Images or texts depicting violence or personal violent crime;
- Images or texts concerning the commissioning of acts of terrorism and the dissemination of the same;
- Images or texts concerning desecration;

The viewing, downloading, storing and/or dissemination of materials, (including cartoons and pseudo photographs) which depict any of the above are to be considered unacceptable uses and are also criminal offences.

There are a number of criminal offences related to accessing, viewing, storing and distribution of pornography, and the exposure of such materials to those under the age of 18 years.

5.2.2 Personal use of Ulster University information and communication equipment and telephony

The University encourages all users to refrain from conducting personal business and from the processing and storage of personal material on University information and communications equipment and telephony; however, the following points should be taken into account if using Ulster University systems or networks for personal use:

- Personal use of any equipment may be withdrawn at any time for operational reasons whether or not it has been subject to abuse;
- The Ulster University accepts no liability for any loss or detriment suffered through personal use of Ulster University information and communications equipment and telephony;
- The Ulster University does not provide a secure transaction system for any information passed, or purchase made, for personal use;
- If you create, send, import or store personal information on any Ulster University system or network, you do so entirely at your own risk and in the knowledge that it may be transferred onto other University systems, may subsequently be accessed by others and that University business processes may result in its loss;
- Any personal materials stored may be accessed when the devices are being maintained or allocated to another user;
- The rules for personal use of official telephones are contained within the University's Finance Regulations. In general, official telephones should not be used for personal calls unless repayment is to be made.

5.2.3 Examples of Unacceptable Use

The list below provides examples of unacceptable use but is not exhaustive. Users are expected to exercise common sense when considering if intended use may be unacceptable. If there is any doubt, users should seek advice from the Information Services Service Desk.

- Users must not endanger, attempt to endanger, or allow the endangerment of Ulster University IT or telecommunications services, or those of other individuals or organizations, which would prevent legitimate access to them, damage them or seek to cause degradation of performance or a denial of service. For example: the deliberate or reckless introduction of any malware or other harmful or nuisance software program or file into any facility. They must not take deliberate action to circumvent any precautions taken or prescribed by the University to prevent such;
- Users must ensure that all machines that connect to the University network have the latest level of anti-virus software and security patches installed. These must be kept up to date;
- Users must not connect to or attempt to connect to restricted access systems or services for which authorisation has not been given; This is known as

hacking and is a criminal offence in terms of the Computer Misuse Act 1990, as amended;

- Users must not act in any way which puts the security of the University's facilities at risk. In particular, user credentials must be kept safe and secure and only used by those authorised to do so;
- Users must not infringe copyright of works in any form including software, documents, images, or audio or video recordings;
- Users must not attempt to conceal or falsify the authorship of any electronic communication;
- Users must not send unsolicited electronic communications to multiple recipients except where it is an authorised communication. Specifically, users must not use facilities to send spam or chain letters;
- Use of University telephony networks to conduct indecent, offensive or abusive calls;
- Users must not access, store or transmit material which can reasonably be considered harassing, insulting, defamatory, promoting violence or promoting any illegal activity;
- Users must not knowingly transmit any data, send or upload any material which promotes discrimination based on race, sex, religion, nationality, political opinion, disability, sexual orientation or age;
- Users must not harm or attempt to harm any person;
- On-line gambling, or any form of betting is prohibited;
- Users must not knowingly transmit, or procure the sending of, any unsolicited or unauthorized advertising or promotional material or any other form of solicitation unless deemed to be necessary in pursuit of core University business.

5.3 ACCEPTABLE USE MONITORING

In the course of normal business, the use of University networks, systems and services is monitored by authorised personnel for the following general purposes:

- To ensure acceptable use;
- To safeguard integrity, security and availability;
- To facilitate capacity planning and optimize performance;
- To assist in fault investigation and incident handling;
- To investigate any suspected or actual breaches of University policy, unauthorised use or criminal activity;

- To gather evidence for investigative or disciplinary purposes;
- To facilitate any other legal and security purposes;

Details of Information Technology Monitoring are contained in the University's IT Monitoring Policy and IT Monitoring Code of Practice.

5.4 COPYRIGHT

Copyright infringement occurs when a person knowingly or unknowingly infringes the exclusive right of the copyright owner to copy, perform, show, play, distribute, adapt, or communicate the work, or rent or lend the work. These are specific "restricted acts" which are exclusive to the copyright owner. The person infringing cannot acquit themselves by correctly attributing the work.

The work of the copyright owner may be used if one of the following applies:

- It has been authorised in writing by the copyright owner;
- It is authorised by the University's licence with the CLA or other licensing agency;
- It is permitted under the statutory exceptions of The Copyright Designs and Patents Act, 1988

For information on copyright visit the University's website at:

www.ulster.ac.uk/copyright

5.5 BREACHES OF THIS CODE OF PRACTICE

Any breach of this Code of Practice may result in disciplinary action. Serious offences may lead to dismissal, suspension or, in the case of Students, expulsion. It shall at all time fall to the discretion of the Ulster University to determine whether there has been any contravention and in particular whether a particular use is acceptable or otherwise.

A breach may result in immediate, temporary or permanent withdrawal of rights to use the University's information and communications equipments and telephony.

Activities which are suspected of being criminal in nature shall, in every case, be reported to the Police Service of Northern Ireland or other appropriate law enforcement agencies.

Any breach of this Acceptable Use Code of Practice may also result in legal proceedings being taken for reimbursement of all costs on an indemnity basis (including, but not limited to, reasonable administrative and legal costs) resulting from the breach.

All users shall follow the "Reporting Unacceptable and Illegal Use" Procedure when reporting such.

Related Standards, Procedures, Guidelines and other documents

1. IT Monitoring Policy;

2. IT Monitoring Code of Practice;
3. Reporting Unacceptable and Illegal Use (Appendix A of this document)

6. Appendix A - Reporting Unacceptable and Illegal Use

This diagram illustrates the steps involved in the process of reporting of unacceptable and illegal usage of University networks, systems and services.