LEGAL FRAMEWORK FOR ICT

COPYRIGHT, INFORMATION GOVERNANCE AND COMPLIANCE

Reviewed 7 September 2018

LEGAL FRAMEWORK FOR ICT

Contents

Introduction

This document should be read in conjunction with the University Policy on the use of Computing Facilities and Resources.

The University of Strathclyde offers Information and Communication Technology to a range of users (staff, students, visitors) to support the teaching, learning, research and administration duties of the University. As a user of the University's ICT systems it is important you are aware of the key legislation that relates to this use.

As legislation and case law in this area is subject to frequent change this document provides a summary and is not an exhaustive list.

You should also be aware that the University's connection to the Internet is provided via JANET (Joint Academic Network) and thus users are bound by the JANET Acceptable Use Policy.

The latest versions of the legislation referred to in this document can be found at: www.legislation.gov.uk/. Note that BREXIT notwithstanding, EU law will continue to apply at least until 29th March 2019.

Legislation

1. Civic Government (Scotland) Act 1982 (as amended by the Criminal Justice and Licensing (Scotland) Act 2010) (equivalent legislation in England and Wales is Obscene Publications Act 1959, Obscene Publications Act 1964 as amended)

The Civic Government (Scotland) Act 1982 (as amended by the Criminal Justice Act 1988, Criminal Justice and Public Order Act 1994 and the Criminal Justice and Licensing (Scotland) Act 2010) makes it an offence to display in a public place, publish, sell or distribute obscene material or (with a view to its eventual sale or distribution) make, print or keep any obscene material which includes a computer disc and any form of recording of a digital image. Where material consists of data stored electronically publishing includes transmitting that data.

It is also an offence to possess an extreme pornographic image which includes data stored by any means which is capable of conversion into such an image.

The same legislation makes it an offence not only to take, permit to be taken, show and distribute but also to possess an indecent photograph or pseudo-photograph of a child. A pseudo-photograph means an image whether made by computer graphics or otherwise, which appears to be a photograph and the term photograph includes a film.

In the event an individual staff member, student or visitor commits any of the aforementioned offences, the individual could face criminal prosecution and the University could suffer reputational damage. There is a defence available where an individual has a legitimate reason for being in possession of an extreme pornographic image or for showing, distributing or being in possession of, an indecent photograph or pseudo-photograph of a child. Therefore, on occasions where access to material covered by the legislation may be required for research purposes, please seek approval from your line manager. You will probably also require to put your proposal through your departmental or the University Ethics committee.

2. Communications Act 2003

The Communications Act 2003 makes it an offence to dishonestly obtain electronic communication services (illegal downloading, file sharing etc.), possess or supply any equipment that may be used for illegally obtaining electronic communications and the improper use of public electronic communications (sending grossly offensive or indecent material, sending a false message for the purpose of annoyance/anxiety to another etc.) See in particular S.127 of the Act.

3. Computer Misuse Act 1990

The Computer Misuse Act 1990 makes it a criminal offence to access, attempt to access or encourage others to access computer material without proper authority or to make unauthorised modifications of computer material. This would include "hacking", the introduction of viruses and knowingly receiving or using material from an unauthorised user who has gained access to computer material.

Image from Pixabay (user iAmMrRob) https://pixabay.com/en/hacking-cyber-blackandwhite-crime-2903156/ 2017 used under CC0 Creative Commons licence

4. Copyright, Designs and Patents Act 1988

The Copyright Designs and Patents Act 1988 and later additional legislation exists to protect the work of authors, creators and performers for a specified period of time during which they are able to control exploitation of their work. Works covered by copyright are original literary, dramatic, musical and artistic works. Items such as broadcasts, sound recordings, films and typographical arrangements of published editions of a literary or dramatic work are also covered. In addition, the recordings of lectures, databases and computer software are dealt with by this area of law.

You may need permission to use the whole or part of someone else's work irrespective of any acknowledgement you give. The fact you may be able to access such a work freely, for example via the internet, does not mean you can necessarily copy, reuse, republish it or send copies to others.

For further information please see the University's Copyright, Information Governance & Compliance webpages.

5. Counter Terrorism and Security Act 2015

The Counter-Terrorism and Security Act 2015 places a duty on universities 'to have due regard to the need to prevent people from being drawn into terrorism'. We expect staff, students and authorised users to comply with the terms of the University Policy on Computing Facilities and Resources when accessing or transmitting information. The University reserves the right to filter and monitor content to prevent users from being drawn into terrorism.

6. Defamation Act 1996

The Defamation Act 1996 and later amendments deal with the protection of an individual's reputation. Defamation law gives an individual whose reputation has been wrongly attacked the right to take legal action against those responsible. The action is normally taken against the publisher of the defamatory statement. This could be the University for specific information published on its website but could also be an individual.

Note there was a further Defamation Act in 2013. Most of its provisions extend only to England and Wales however S.6 which provides for a defence of qualified privilege in relation to statements in a peer reviewed scientific or academic journal does apply in Scotland.

7. Environmental Information (Scotland) Regulations 2004

Environmental Information (Scotland) Regulations 2004 (EIRs) come from a European Directive on access to environmental information. The EIRs aim to promote the release of environmental information to the public and give everyone the right to ask for environmental information held by a Scottish public authority including universities.

8. Equality Act 2010

The Equality Act 2010 applies to all public authorities and covers the following protected characteristics: age, disability, sex, gender reassignment, pregnancy and maternity, race, religion/belief, marriage and civil partnership and sexual orientation. The University must have due regard to the need to eliminate unlawful discrimination, harassment and victimisation, and advance equality of opportunity between those who share protected characteristics and those who do not. Individual staff and students must also comply with this legislation. For further information please see the University's Equality and Diversity webpages.

9. Freedom of Information (Scotland) Act 2002

The Freedom of Information (Scotland) Act 2002 [FOISA] gives individuals the right to receive recorded information held by Scottish public authorities, including universities, subject to certain exemptions. The Act aims to promote openness and accountability across the public sector. For further information on the Freedom of Information (Scotland) Act and the associated handling and communication of data see the University's Freedom of Information webpages.

10. General Data Protection Regulation (EU) 2016/679 and Data Protection Act 2018

The General Data Protection Regulation (GDPR) is a new EU legal framework for data protection which (together with the Data Protection Act 2018) replaces the Data Protection Act 1998. GDPR applies to all member states and introduces some new obligations for organisations that collect, use, share and store personal data.

https://openclipart.org/detail/302584/gdpr Open Clip Art by Onsemeliot 2018

GDPR is based on 6 basic principles. The University has a legal duty to act in accordance with these principles when collecting, processing, storing and destroying personal data in order to ensure personal data is

- processed fairly and lawfully,
- collected for specified, explicit and legitimate purposes,
- limited to what is necessary for the purposes for which it is processed,
- accurate and kept up to date
- kept for no longer than is necessary
- processed in a manner that ensures appropriate security of the personal data

The Act applies to individual staff and students if they undertake processing of personal data. For example library staff may need to process personal data in order to deal with enquiries from staff or students, staff in Human Resources will require to process personal information about staff in the course of their duties and academic staff or students may be processing personal data in the course of research. For further information please see the University's Data Protection webpages . Note GDPR came into force on 25th May 2018 therefore it will apply to the UK irrespective of BREXIT in 2019.

11. Human Rights Act 1998

The Human Rights Act 1998 is a fundamental piece of legislation that applies to all UK citizens which government and public authorities (including universities) are legally obliged to respect. The Act sets out a number of basic rights and freedoms contained in the European Convention on Human Rights (ECHR) 1950. The rights impact on matters of equality, dignity and respect, and individual staff and students should always keep this in mind in their work and dealings with others.

12. Investigatory Powers Act 2016, Regulation of Investigatory Powers (Scotland) Act 2000 & The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-Keeping Purposes) Regulations 2018

The Investigatory Powers Act 2016 which applies in Scotland and the rest of the UK replicates and consolidates existing provisions (including within Regulation of Investigatory Powers (Scotland) Act 2000) making it a criminal offence to undertake the interception of communications in the UK without legal authority. The Act also sets out what constitutes 'lawful authority' to conduct interception.

Whether, and to what extent, the University can monitor or record communications within their telecommunication system is governed by this legislation.

There are two areas where the interception of communications by the University is lawful. These are:

- Where the University reasonably believes that the sender and intended recipients have consented to the interception.

- Where the University monitors or keeps a record of communications for the purposes set out in The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-Keeping Purposes) Regulations 2018. These purposes include:
    - To ensure compliance with regulatory practices or procedures
    - To prevent or detect a crime
    - To investigate or detect the unauthorised use of the telecommunication system
    - To secure the effective operation of the telecommunication system

The University does not need to gain consent before intercepting for the purposes set out in the Regulations. However the University is expected to make reasonable efforts to inform staff, students or any other person who may use the telecommunication system that communications transmitted by means of that system may be intercepted.

13. Modern Slavery Act 2015 and Human Trafficking and Exploitation (Scotland) Act 2015

The Modern Slavery Act 2015 provides law enforcement with tools to fight modern slavery which takes various forms such as slavery, servitude, forced and compulsory labour and human trafficking all of which involve the deprivation of a person's liberty by another in order to exploit them for personal or commercial gain. Modern slavery is a crime and a violation of human rights.

The Modern Slavery Act 2015 mostly covers England and Wales however the equivalent offences in Scotland are covered by the Human Trafficking and Exploitation (Scotland) Act 2015 and certain provisions of the Modern Slavery Act 2015, in particular the requirement to prepare and publish a slavery and human trafficking statement, apply in Scotland.

The University's Modern slavery and human trafficking statement is available on the University website.

The University has an obligation to take steps to ensure that modern slavery and human trafficking is not taking place in any part of its operation within the University and its supply chain. These

obligations are embedded in the University's Supply Chain Code of Conduct which underpins all tendering activities including procurement of ICT products and services.

14. Terrorism Act 2006

The Terrorism Act 2006 makes it an offence to encourage terrorism and to distribute terrorism material through any media. The Act allows the police the right to serve a take-down notice on any providers of electronic communications to remove any material that directly or indirectly promotes terrorism.

Other relevant Policies and Guidance

1. JANET Acceptable Use

Users of the University's IT system must comply with the JANET (Joint Academic Network) policies on acceptable use and security including:

JANET Acceptable Use Policy

JANET Security Policy

2. Social Media

The use of social media platforms can have some legal issues associated with them. Please see the University Guidance on the Use of Social Media for further information.

3. Bring Your Own Device

The University of Strathclyde recognises the benefits that can be achieved by allowing staff to use their own electronic devices when working whether that is at home, on campus or while travelling. Such devices include laptops, smart phones and tablets and the practice is commonly known as 'bring your own device' or BYOD. It is committed to supporting staff in this practice however the University recognises that there are risks involved in particular in the area of information security. Staff should be aware that they are responsible for acting in compliance with the law when using their own devices for work and must comply with relevant University policies including the University Bring Your Own Device Policy.

Further Information

For information on Freedom of Information please contact: foi@strath.ac.uk

For information on Data Protection please contact dataprotection@strath.ac.uk

For all other enquiries please contact: ICTlegalcompliance@strath.ac.uk