## Acceptable use of computing facilities policy

<table>
<thead>
<tr>
<th>Document Filename</th>
<th>Acceptable Use Policy.docx</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1.0</td>
</tr>
<tr>
<td>Information Classification</td>
<td>Open</td>
</tr>
<tr>
<td>Status</td>
<td>Approved</td>
</tr>
<tr>
<td>Date</td>
<td>18 December 2015</td>
</tr>
<tr>
<td>Policy owner</td>
<td>Graham McKay</td>
</tr>
<tr>
<td>Policy contact</td>
<td><a href="mailto:g.mckay@dundee.ac.uk">g.mckay@dundee.ac.uk</a></td>
</tr>
</tbody>
</table>
## Document Approval

<table>
<thead>
<tr>
<th>Title/Role</th>
<th>Name of Approver(s)</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Management Committee</td>
<td>Jim McGeorge, Paul Saunders, Ian Leith, Richard Parsons, Wesley Rennison, Andrew Hewitt, Tim Hustler.</td>
<td>18/12/2015</td>
</tr>
</tbody>
</table>

## Version Control

<table>
<thead>
<tr>
<th>Revision</th>
<th>Status</th>
<th>Author(s)</th>
<th>Reviewed By</th>
<th>Approved By</th>
<th>Issue Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Draft</td>
<td>Graham McKay</td>
<td></td>
<td></td>
<td>01/09/2015</td>
</tr>
<tr>
<td>0.2</td>
<td>Draft</td>
<td>Graham McKay</td>
<td>Richard Parsons</td>
<td>Alan Bell</td>
<td>07/09/2015</td>
</tr>
<tr>
<td>1.0</td>
<td>Approved</td>
<td>Graham McKay</td>
<td>Richard Parsons</td>
<td>Alan Bell, Information Management Committee</td>
<td>18/12/2015</td>
</tr>
</tbody>
</table>
Contents
1 Document overview ........................................................................................................... 1
  1.1 Purpose ......................................................................................................................... 1
  1.2 Scope ............................................................................................................................ 1
  1.3 Definitions ..................................................................................................................... 1
  1.4 References .................................................................................................................... 1
2 Policy .................................................................................................................................. 2
3 Review .................................................................................................................................. 3
4 Breaches of policy ............................................................................................................... 3
5 Further information ......................................................................................................... 3
6 Guidance ............................................................................................................................. 4
  6.1 This policy has been directed by the following legislation: ........................................ 4
  6.2 Obscene Publications Act 1959 ..................................................................................... 4
  6.3 Copyright, Designs and Patents Act 1988................................................................. 4
  6.4 Criminal Justice and Courts Act 2015 ........................................................................ 4
  6.5 Computer Misuse Act 1990 ....................................................................................... 4
  6.6 Criminal Justice Act 1988 ........................................................................................... 4
  6.7 Criminal Justice Public Order Act 1994 ................................................................. 5
  6.8 Defamation Act 1996 .................................................................................................. 5
  6.9 Data Protection Act 1998 ............................................................................................ 5
  6.10 Human Rights Act 1998 ............................................................................................ 5
  6.13 Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ......................................................................................... 6
  6.14 Terrorism Act 2006 .................................................................................................. 6
  6.15 Equality Act 2010 .................................................................................................... 6
  6.16 Counter Terrorism and Security Act 2015 ............................................................. 6
  6.17 Further guidance ....................................................................................................... 6
1 Document overview

1.1 Purpose

1.1.1 The purpose of this policy is to outline the acceptable use of computing facilities at the University of Dundee. This policy has been formulated with the following objectives in mind:

- To ensure confidentiality, integrity and availability of our computing facilities;
- To protect individuals and the organisation from liability;
- To maintain our image and reputation; and
- To preserve the privacy and security of our users.

1.2 Scope

1.2.1 This policy covers the use of all University computer facilities, systems and networks and is applicable to all staff, students and visitors.

1.3 Definitions

1.3.1 University – The University of Dundee is a Scottish Registered Charity, No. SC01509 with its registered office at Tower Building, Nethergate, Dundee DD1 4HN.

1.3.2 Staff - Staff are salaried members of the University or contracted individually by the University to provide a service.

1.3.3 Student - a person pursuing any course of study in the University.

1.3.4 Visitors - A visitor is anyone, not a member of staff or student, requiring access to University premises or services.

1.3.5 Confidentiality\(^1\) - property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

1.3.6 Integrity\(^2\) – property of accuracy and completeness.

1.3.7 Availability\(^3\) – property of being accessible and usable upon demand by an authorized entity.

1.4 References

1.4.1 Policy Exemption request process.

---

\(^1\) ISO/IEC 27000:2014 - 2.12
\(^2\) ISO/IEC 27000:2014 - 2.40
\(^3\) ISO/IEC 27000:2014 - 2.9
2 Policy

2.1.1 The computing facilities provided by the University of Dundee may not be used for:

- any immoral, unlawful or unethical purpose;
- anything which violates established practice or protocols on the Internet;
- for personal use
  - which significantly affect the performance or availability of computing services; or
  - which affects your ability to carry out your role; or
  - which affects your ability to undertake your course of study.

2.1.2 Where you are expressly required to undertake any of the above in the course of your role either for academic or research purposes, you are required to complete a Security Exception request form, which must be authorised prior to access.

2.1.3 When a computer or laptop is supplied by the University, it is loaded with the properly licensed software required and managed. No software other than that available from the software store should be added without prior permission of UoD IT.
3 Review

3.1.1 The Information Security Steering Group is responsible for keeping this policy current. This policy will be reviewed annually or more frequently as required.

4 Breaches of policy

4.1.1 Failure to comply with this policy may result in disciplinary action being taken against you under University of Dundee disciplinary procedures, which may include summary dismissal. If there is anything in this policy that you do not understand, please discuss it with your line manager.

5 Further information

5.1.1 If you have any questions regarding this policy, please contact the Chief Information Security Officer at g.mckay@dundee.ac.uk.
6 Guidance

6.1 This policy has been directed by the following legislation:

6.2 Obscene Publications Act 1959

6.2.1 The law makes it an offence to publish, whether for gain or not, any content whose effect will tend to "deprave and corrupt" those likely to read, see or hear the matter contained or embodied in it. This could include images of extreme sexual activity such as bestiality, necrophilia, rape or torture.

6.2.2 The Sex Discrimination Act 1975, Race Relations Act 1976 and Disability Discrimination Act 1995 make it an offence to discriminate on the grounds of sex, race or disability (or perceived disability). Harassment, such as unwelcome emails or copying of such material from the Internet, is not permitted and could result in legal action against you.

6.3 Copyright, Designs and Patents Act 1988

6.3.1 Copyright is a legal means of ensuring that content creators can protect what they create. When using computers, unless you have permission with regard to a particular copyrighted material, it is illegal to:

- make copies
- publish
- distribute
- sell copies

6.3.2 If you download a music track, film, game or programme without the copyright holder's permission, you are breaking the law.

6.4 Criminal Justice and Courts Act 2015

6.4.1 Offences created under this act include meeting a child following sexual grooming and possession of pornographic images of rape and assault by penetration.

6.5 Computer Misuse Act 1990

6.5.1 The Computer Misuse Act attempts to discourage people from using computers for illegal purposes. There are three separate parts to the Act:

6.5.2 It is illegal to access data stored on a computer unless you have permission to do so.

6.5.3 It is illegal to access data on a computer when that material will be used to commit further illegal activity, such as fraud or blackmail.

6.5.4 It is illegal to make changes to any data stored on a computer when you do not have permission to do so. If you access and change the contents of someone’s files without their permission, you are breaking the law. This includes installing a virus or other malware which damages or changes the way the computer works.

6.6 Criminal Justice Act 1988
6.6.1 Offences created under this act include possession of indecent photograph of child.

6.7 Criminal Justice Public Order Act 1994

6.7.1 Offences created under this act include offences related to Obscene publications and indecent photographs of children.

6.8 Defamation Act 1996

6.8.1 It is unlawful to make an untrue statement, published to a third party, which damages the reputation of a person or company or holds them up to hatred, ridicule or contempt. It need not be obviously insulting. It could, for example, be a suggestion that a competitor is in financial difficulties or is unprofessional in the conduct of its business. Facts concerning individuals or organisations must be accurate and verifiable and views or opinions must not portray their subjects in any way that could damage their reputation.

6.9 Data Protection Act 1998

6.9.1 The Data Protection Act exists to protect personal details and encompasses eight principles which state how personal data should be treated:

- Personal data must be fairly and lawfully processed
- Personal data must be obtained for specified and lawful purposes.
- Personal data must be adequate, relevant and not excessive.
- Personal data must be accurate and up to date
- Personal data must not be kept for longer than is necessary.
- Personal data must be processed in line with our rights. Your rights include the right to see any data held on you, and the right to correct inaccurate data.
- Personal data must be held securely.
- Personal data must not be transferred to other countries outside the European Economic Area, unless those countries have similar data protection laws.

6.10 Human Rights Act 1998

6.10.1 This act includes the right of an individual to privacy of communications.


6.11.1 These acts provide a right to receive information from public authorities.


6.12.1 These acts enable relevant permitted investigatory powers to be used in accordance with human rights covering

- the interception of communications
- the acquisition of communications data (e.g. billing data)
- intrusive surveillance (on residential premises/in private vehicles)
- covert surveillance in the course of specific operations
• the use of covert human intelligence sources (agents, informants, undercover officers)
• access to encrypted data

6.13 Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

6.13.1 Allows businesses, including Public Authorities, to intercept communication on their own telecommunications network without consent, for certain specified purposes.

6.14 Terrorism Act 2006

6.14.1 This act makes it an offence “to collect material which could be used by a person committing or preparing for an act of terrorism.”

6.15 Equality Act 2010

6.15.1 The Equality Act replaced previous anti-discrimination laws with a single act (The Sex Discrimination Act 1975, Race Relations Act 1976 and Disability Discrimination Act 1995) and makes it an offence to discriminate on the grounds of sex, race or disability (or perceived disability).

6.16 Counter Terrorism and Security Act 2015

6.16.1 This act imposes a duty on “specified authorities” – if which the University is one -, when exercising their functions, to have due regard to the need to prevent people from being drawn into terrorism.

6.17 Further guidance

6.17.1 For the avoidance of doubt, viewing, accessing, transmitting, posting, downloading or uploading any of the following materials are strictly prohibited (this list is not exhaustive):

• material which is sexist, racist, homophobic, xenophobic, pornographic, paedophilic or similarly discriminatory and/or offensive;
• offensive, obscene, derogatory or criminal material or material which is liable to cause embarrassment to the University and any of its staff, students or stakeholders or bring the reputation of the University and any of its staff or its customers into disrepute;
• any defamatory material about any person or organisation or material which includes statements which are untrue or of a deceptive nature;
• any material which violates the privacy of others or unfairly criticises or misrepresents others;
• any other statement which is likely to create any liability (whether criminal or civil, and whether for you or the University);
• material in breach of copyright and/or other intellectual property rights; or
• unsolicited commercial or advertising material, chain letters or other junk mail of any kind.