ICT Acceptable Use Policy

Quick Summary

1. You must not use anything that you are not permitted to access.
2. You must not do anything illegal.
3. You must not create or use offensive material.
4. You must not introduce viruses or do anything else that causes problems for others.
5. Do not email or remove any Personal or Confidential data without obtaining permission and using strong encryption.
6. You could be subject to disciplinary and/or other action if you break the rules.
7. If you are not sure about anything contact the ICT Service Desk on x6500 or helpdesk@lincoln.ac.uk.

Author
Mark N R Smith, ICT Services

Approved
D Cook

Current Version
2.06

Issue Date
22.07.2014

Review Date
22.07.2017
## Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author(s)</th>
<th>Notes on Revisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>11.09.09</td>
<td>Mark Smith</td>
<td>Version 1 issued.</td>
</tr>
<tr>
<td>1.1</td>
<td>15.10.09</td>
<td>Mark Smith</td>
<td>Added unintentional email clause &amp; clarified investigation &amp; monitoring provision.</td>
</tr>
<tr>
<td>1.2</td>
<td>30.11.09</td>
<td>Mark Smith, Mike Day</td>
<td>Further investigation and monitoring clarification.</td>
</tr>
<tr>
<td>1.3</td>
<td>11.12.09</td>
<td>Mark Smith</td>
<td>Typo and section 4 privacy paragraph.</td>
</tr>
<tr>
<td>1.4</td>
<td>10.06.10</td>
<td>Mark Smith</td>
<td>Added PCI-DSS requirements.</td>
</tr>
<tr>
<td>1.5</td>
<td>27.07.11</td>
<td>Mark Smith</td>
<td>Data Protection and Mobile improvements</td>
</tr>
<tr>
<td>1.51</td>
<td>21.09.11</td>
<td>Mark Smith</td>
<td>Comments from Ann-Marie Noble</td>
</tr>
<tr>
<td>1.52</td>
<td>22.09.11</td>
<td>Mark Smith</td>
<td>Further comments from Ann-Marie Noble</td>
</tr>
<tr>
<td>1.53</td>
<td>03.10.11</td>
<td>Mark Smith</td>
<td>ICT Security Group Comments</td>
</tr>
<tr>
<td>1.54</td>
<td>15.12.11</td>
<td>Mark Smith</td>
<td>Discussions with LH</td>
</tr>
<tr>
<td>2.00</td>
<td>11.05.12</td>
<td>Mark Smith</td>
<td>Version 2 issued</td>
</tr>
<tr>
<td>2.01</td>
<td>13.06.12</td>
<td>Mark Smith</td>
<td>Added research ethics committee to 4.1.10, corrected section numbers and reissued.</td>
</tr>
<tr>
<td>2.02</td>
<td>4.12.13</td>
<td>Mark Smith</td>
<td>New template</td>
</tr>
<tr>
<td>2.03</td>
<td>4.12.13</td>
<td>Mark Smith</td>
<td>Minor improvements, PCI-DSS and offsite printing</td>
</tr>
<tr>
<td>2.04</td>
<td>18.12.13</td>
<td>Mark Smith</td>
<td>Amended title</td>
</tr>
<tr>
<td>2.05</td>
<td>15.07.14</td>
<td>Mark Smith</td>
<td>Added Office 365 as approved cloud provision;</td>
</tr>
<tr>
<td>2.06</td>
<td>22.07.14</td>
<td>Mark Smith</td>
<td>Version 2.06 issued</td>
</tr>
</tbody>
</table>

## Approval

This document has been approved by:

D Cook – Director of ICT
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>1.1</td>
<td>Purpose of Policy</td>
<td>4</td>
</tr>
<tr>
<td>1.2</td>
<td>Policy Objectives</td>
<td>4</td>
</tr>
<tr>
<td>1.3</td>
<td>Help with this Policy</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>Scope</td>
<td>6</td>
</tr>
<tr>
<td>2.1</td>
<td>Who is covered by this policy?</td>
<td>6</td>
</tr>
<tr>
<td>2.2</td>
<td>What ICT Resources are covered by this policy?</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>General Guidelines</td>
<td>7</td>
</tr>
<tr>
<td>3.1</td>
<td>Principles of this Policy</td>
<td>7</td>
</tr>
<tr>
<td>3.2</td>
<td>Disclaimer</td>
<td>9</td>
</tr>
<tr>
<td>4</td>
<td>Email Use</td>
<td>10</td>
</tr>
<tr>
<td>4.1</td>
<td>Introduction</td>
<td>10</td>
</tr>
<tr>
<td>4.2</td>
<td>Email Usage</td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td>Software, Services - Applications and Data</td>
<td>12</td>
</tr>
<tr>
<td>5.1</td>
<td>Introduction</td>
<td>12</td>
</tr>
<tr>
<td>5.2</td>
<td>Software, Services - Applications and Data Usage</td>
<td>12</td>
</tr>
<tr>
<td>6</td>
<td>Internet and Networks</td>
<td>14</td>
</tr>
<tr>
<td>6.1</td>
<td>Introduction</td>
<td>14</td>
</tr>
<tr>
<td>6.2</td>
<td>Internet Usage</td>
<td>14</td>
</tr>
<tr>
<td>7</td>
<td>Mobiles, Laptops, Tablets and Portable Storage</td>
<td>16</td>
</tr>
<tr>
<td>7.1</td>
<td>Introduction</td>
<td>16</td>
</tr>
<tr>
<td>7.2</td>
<td>Use of Mobiles, Laptops, Tablets and Portable Storage</td>
<td>16</td>
</tr>
<tr>
<td>8</td>
<td>Remote Access Working</td>
<td>18</td>
</tr>
<tr>
<td>8.1</td>
<td>Introduction</td>
<td>18</td>
</tr>
<tr>
<td>8.2</td>
<td>Remote Access Usage</td>
<td>18</td>
</tr>
<tr>
<td>9</td>
<td>Compliance</td>
<td>19</td>
</tr>
<tr>
<td>9.1</td>
<td>Applicable Compliance Legislation</td>
<td>19</td>
</tr>
<tr>
<td>9.2</td>
<td>Email Access, Investigation and Monitoring Provisions</td>
<td>19</td>
</tr>
<tr>
<td>10</td>
<td>Policy Violations</td>
<td>21</td>
</tr>
<tr>
<td>10.1</td>
<td>Reporting Policy Violations</td>
<td>21</td>
</tr>
<tr>
<td>10.2</td>
<td>Consequences of Policy Violations</td>
<td>21</td>
</tr>
<tr>
<td>11</td>
<td>Relevant Documents</td>
<td>22</td>
</tr>
<tr>
<td>11.1</td>
<td>Other Documents</td>
<td>22</td>
</tr>
<tr>
<td>11.2</td>
<td>Document Locations</td>
<td>22</td>
</tr>
<tr>
<td>12</td>
<td>Useful Contacts</td>
<td>22</td>
</tr>
<tr>
<td>12.1</td>
<td>Useful Contacts</td>
<td>22</td>
</tr>
<tr>
<td>13</td>
<td>Agreement for External Parties</td>
<td>23</td>
</tr>
</tbody>
</table>
1 Introduction

1.1 Purpose of Policy

This document defines the University of Lincoln’s Information and Communications Systems Acceptable Use Policy for Information and Communication Technology (ICT) Resources.

The ICT Resources provided for academic purposes and University business are extremely valuable assets which are relied upon for the delivery of University service.

This policy is designed to support all areas of the University’s business and to recognise academic freedoms when using ICT Resources.

The intention is that this policy will enable the University to carry out its activities, by protecting and preserving University ICT Resources at the appropriate level.

The policy is intended to protect the ICT assets of the University by adopting the core principles of information security:

- **Confidentiality** – the prevention of unauthorised disclosure of information;
- **Integrity** – the prevention of corruption or unauthorised amendment or deletion of information;
- **Availability** – the prevention of unauthorised withholding of information or resources.

This policy has been subjected to an Equality Impact Assessment. During the screening process it was judged to not to disproportionately affect any equality group. This is because the policy defines a protocol for everybody which outlines behaviour when using ICT resources. Therefore no further Equality Impact Assessment process is required.

1.2 Policy Objectives

The objectives of the policy are:

- To ensure users have proper awareness and concern for the security of ICT resources and adequate appreciation of their responsibilities during its use;
- To provide guidance for the acceptable use of ICT Resources;
- To ensure that users are aware of their legal obligations when using ICT resources;
- To ensure users are aware of their accountability and aware that failure to abide by this policy is a disciplinary matter which may have serious consequences under the terms of University Regulations, Contracts of Employment or other contracts or agreements. Ultimately, this could result in summary expulsion, dismissal or cancellation of contract or agreements.
1.3 Help with this Policy

Guidance and clarification about the interpretation or any other aspect of this policy is available through the ICT Service Desk that can be contacted on x6500 or helpdesk@lincoln.ac.uk.

If you feel that your particular requirements for use of ICT Resources have not been properly addressed by this policy please contact the ICT Service Desk on x6500. When difficult issues arise, particularly with academic requirements, they may be referred to the appropriate University ethics committee.
2 Scope

This section sets out what this Acceptable Use Policy covers.

2.1 Who is covered by this policy?

This policy applies to people, denoted as ‘users’ in this Policy, using the University of Lincoln ICT Resources in section 2.2, including, but not limited to:

- Students enrolled at the University;
- Permanent staff employed by the University;
- Temporary, casual or agency staff working for, or on behalf of, the University;
- Contractors, consultants and suppliers working for, or on behalf of, the University;
- Visitors to the University.

2.2 What ICT Resources are covered by this policy?

This policy applies to ICT Resources and systems made available for use by users by, or on behalf of, the University of Lincoln, including but not limited to:

- PCs including desktop PCs, Apple Macs or other Apple computers, laptop PCs and terminals;
- Peripherals e.g. printers, copiers and scanners;
- Mobile devices, including smartphones, tablets, iPods, PDAs (Personal Digital Assistants), telephones, mobiles and other ‘smart’ devices;
- Networks with wired, wireless, dialup and/or internet connections;
- Internet services including the world wide web, blogs and wikis;
- Email and other messaging, social networking or collaboration services e.g. blogs, chat, forums, Facebook, Twitter, YouTube, MySpace, bebo etc.;
- Application software, services and data including databases;
- Removable media, such as CDs, DVDs and memory sticks.
3 General Guidelines

3.1 Principles of this Policy

When using ICT Resources users are expected to comply with the letter and the spirit of this Policy and specifically:

1. You must not use any ICT Resource that you are not permitted to access.

2. You must not break English law or breach any University Policy or Regulation (including but not limited to policies or regulations covering such areas as harassment and discrimination).

3. You must not display, store, transmit or knowingly receive images, text or any other material which could be considered illegal, paedophilic or defamatory (see section 10 to report receiving such material).

4. You must not display, store, transmit or knowingly receive images, text or any other material which could be considered indecent, obscene, pornographic or of a terrorist nature unless you have a legitimate reason for doing so and have written authorisation from your academic supervisor or head of department (see section 10 to report receiving such material).

5. You must not display, store, transmit or knowingly receive images, text or any other material which is, or could be considered as, discriminatory, offensive, abusive, racist or sexist when the context is a personal attack or might be considered harassment (see section 10 to report receiving such material).

6. You must not engage in behaviour that damages or adversely affects any University ICT Resources or damages or adversely affects the ability of other users to use the University ICT Resource.

7. You must not use any ICT Resource in a way that brings, or may bring, the University into disrepute.

8. You must not compromise or risk compromising the security, confidentiality, availability or integrity of the University’s ICT Resources in any way whatsoever.

9. Staff must ONLY enter (or direct others to enter) Credit/Debit card numbers and associated security codes into approved PCI-DSS compliant payment collection devices, e.g. approved tills and PDQ devices, or approved online payment collection applications and web interfaces using secure and approved computers. Credit/Debit card numbers and associated security codes should NEVER be written down on paper, typed into emails, stored in spreadsheets or other documents, or entered into non approved ICT systems.

10. You must take appropriate care when using Personal or Confidential information and abide by the UK Data Protection Act (1998).

Personal data is defined as data which identifies a living person and includes sensitive Personal data. Examples of Personal data include:
a) National Insurance Number or similar reference numbers (e.g. passport number).
b) Combination of name, date of birth or personal contact details. 
   Personal contact details include home address, personal email address, 
   home phone number and personal mobile number;

Sensitive Personal Data is defined as data as to the persons:

a) Racial or ethnic origin;
b) Political opinions;
c) Religious beliefs or other beliefs of a similar nature;
d) Membership of a trade union;
e) Physical or mental health or condition;
f) Sexual life (e.g. sexual orientation);
g) Details of any offenses or court proceedings;

Appropriate care when using Personal data means; using appropriate technical 
and organisational measures to prevent unauthorised or unlawful processing 
and to prevent accidental loss or damage to the information. See Section 
5.2.10 for more details about the legal obligations when handling Personal 
data.

Confidential data is defined as data which if it became public would cause 
significant financial or reputational damage to the University. This includes 
amongst other things):

a) Bank account details or similar financial information (e.g. bank account 
   numbers);

If you need help or clarification you must seek appropriate advice from your 
supervisor/line manager or the ICT Service Desk (x6500 or 
helpdesk@lincoln.ac.uk).

Any staff or students who may be involved in research, professional practice, 
or other activities that requires them to process, or have access to personal 
data as defined within the data protection policy, confidential data (either 
relating to the University of Lincoln, or its partners), or material that is illegal, 
indecent, obscene, pornographic, related to terrorism, related to extreme 
political views, or may be considered offensive, must first refer the requested 
activity to the research ethics committee, or other appropriate authority 
within the University.

11. You must not knowingly introduce malicious software, such as viruses or 
similar threats, into any University ICT Resource or other ICT Resource.

12. You must not use any ICT Resource in contravention of any applicable license 
agreements or copyright obligations.

13. Not to use another user’s identity or otherwise disguise their identity when 
using any ICT Resource.

14. You must not use an ICT Resource for any unauthorised commercial purpose.

15. External organisations or users that contract to abide by this policy agree to 
ensure that their partners and subcontractors also contract to abide by this
policy as a condition of their partners or subcontractors using ICT Resources covered by this policy.

16. If you require changes to an ICT Resource, such as changing its location, you must consult the ICT Service Desk on x6500 or helpdesk@lincoln.ac.uk.

17. If you do not consider yourself competent using the ICT resource you must seek appropriate advice e.g. the ICT Service Desk on x6500 or helpdesk@lincoln.ac.uk.

### 3.2 Disclaimer

The University will not be liable, beyond any statutory liability, for any loss, damage or inconvenience arising directly or indirectly from the use of, or prevention of use of, any ICT resource.

The University also accepts no liability, beyond any statutory liability, for any ICT material submitted to or processed on any ICT resource. Similarly the University also accepts no liability, beyond any statutory liability, for any ICT material deposited at or left on University premises.
4 Email Use

4.1 Introduction

The University promotes and encourages the use of email as an important means of communication and to provide an efficient method of conducting the University’s business. However, misuse of this facility can have a negative impact upon the work and reputation of the University.

Users may be given access to University email systems for the conduct of University-related business. The use of email facilities is subject to this policy as well as all relevant laws and other University Policies and Regulations.

Although most people use email for University business, reasonable and sensible personal use of email is permitted as long as it does not disrupt or distract the user from the conduct of University business (e.g. due to volume, frequency or time expended).

Similarly personal use of email should not restrict the use of email by other legitimate users. Care should be taken to ensure that email is addressed to the correct business or personal recipient. If you receive an email for which you are not the intended recipient please notify the sender immediately and remove it from your system. Do not disclose the contents to another person or take copies.

The contents of personal emails are private and their contents are not investigated or monitored except in the limited and exceptional circumstances set out in section 9.2. It is recommended that personal email be marked personal in the subject line and stored in a separate folder.

The nature of the internet means that email is inherently insecure and users should assume that email information is not secure or protected while in transit (unless it is encrypted using an appropriate method).

The University provides anti-virus and spam (unsolicited email) filtering services as a matter of course to users of the email service.Whilst efforts are made to keep these filtering services effective and up-to-date, the University can provide no guarantee that they will be effective against all viruses or spam.

Under some limited circumstances the University may access and disclose the contents of email messages in accordance with its legal and audit obligations and for legitimate operational purposes. See section 9 for more information.

4.2 Email Usage

The University’s email resources must not be used for:

1. Distributing or storing images, text or materials that are, or might be considered as, illegal, paedophilic or defamatory.

2. Distributing or storing images, text or materials that are, or might be considered as, indecent, obscene, pornographic or of a terrorist nature unless
you have a legitimate reason for doing so and have written authorisation from your academic supervisor or head of department.

3. Distributing or storing images, text or materials that are, or might be considered as, discriminatory, offensive, abusive, sexist or racist when the context is a personal attack or might be considered as harassment.

4. Knowingly introducing malicious software, such as a virus or similar threat, into the University ICT Resources or the ICT resources of any other person or organisation.

5. Sending or deliberately receiving Credit or Debit Card numbers (see 3.1.9 for definition). If you do receive an email containing a Credit or Debit card number you must delete it immediately.

6. Sending emails that are unrelated to the business of the University (except for limited personal use mentioned in the introduction above) or for personal gain.

7. Sending commercial material or software or any copyrighted material belonging to parties outside of the University, or belonging to the University itself, without legitimate permission from the owner.

8. Sending unsolicited email (‘spam’), chain letters or any form of unauthorised or unsolicited content using University email resources.

9. Sending unsolicited email (‘spam’) to a large number of recipients without authorisation e.g. sending to email groups, such as faculties or departments that the sender is not a member of, or sending to all students or all staff. (Contact the Communications Department or ICT to send to all staff or all students or to use the ‘Daily Alert’ service for this type of communication.)

10. Impersonate or otherwise disguise identity (‘spoof’) when using University email resources.

11. When sending Personal or Confidential information (see 3.1.10 for definition) by email externally (i.e. not to an address with a ‘@lincoln.ac.uk’ suffix) you must have authorisation from your supervisor or line manager and it must be strongly encrypted (the ICT Service Desk on x6500 or helpdesk@lincoln.ac.uk can advise on this). The password must be transmitted to the recipient by an alternative method (e.g. by telephone).

12. Sending Personal or Confidential information (see 3.1.10 for definition) without properly assessing the risks involved.

13. If the information is sent externally (see 4.2.11 above), relates to many individuals or contains Sensitive Personal information or is sent to many people then it must be encrypted. The encryption password must be transmitted to the email recipient by an alternative method (e.g. by telephone). The ICT Service Desk on x6500 or helpdesk@lincoln.ac.uk can advise on this.
5 Software, Services - Applications and Data

5.1 Introduction

The University provides software, applications and services through a variety of delivery platforms enabling users to carry out the business of the University.

Users are required to ensure that they have appropriate authorisation when using any software, service, application or data.

Users are permitted to use applications or services only within the provisions of applicable licensing agreements and copyright obligations.

The University requires that only authorised software, services, applications or data are used with its ICT Resources. Users should not use or install unlicensed software including, but not limited to, applications, utilities, services or leisure software (e.g. music, films, games) on ICT Resources.

Users must process and handle information in accordance with the UK Data Protection Act (1998).

5.2 Software, Services – Applications and Data Usage

When using software, applications, services or data the user must:

1. Be properly authorised to access the software, service, application or data by the appropriate authority and not facilitate unauthorised access by others.

2. Not engage in behaviour that adversely affects the ability of other users to use any software, service, application or data.

3. Not disclose to others (except under special circumstances – see Monitoring section below), their University login name/password combination(s).

   *** Note: the ICT Service Desk will NEVER request your password ***

4. Not to use another user’s identity, appear anonymous or otherwise disguise their identity, or facilitate these actions (for example, by leaving an unattended PC unlocked) when using the software service, application or data requiring proper identification.

5. Not copy any software, service, application or data without legitimate authorisation.

6. Enter or save a Credit or Debit card number (see 3.1.9 for definition) in a University application or service OR enter or save a Credit or Debit card number in University data. The exception to this is when paying by Debit or Credit card using an authorised University secure payment service.

7. Not to allow sensitive data (see section 7 for definition) to physically travel, or be transmitted via an external network (i.e. outside the University), without authorisation from your supervisor or line manager. A secure transfer
mechanism using strong encryption must be used (advice is available via the ICT Helpdesk).

8. Not alter or change the operation of any software service, application or data to facilitate the circumvention of any aspect of this, or any other University policy.


10. When handling Personal data (see section 3.1.10 for definition) abide by UK Data Protection Act (1998) including the eight principles of:

   - Personal data shall be processed fairly and lawfully;
   - Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or purposes;
   - Personal data shall be adequate, relevant and not excessive in relation to the purposes or purposes for which they are processed;
   - Personal data shall be accurate and, where necessary, kept up to date;
   - Personal data processed for any purpose shall not be kept for any longer than is necessary for that purpose or those purposes;
   - Personal data shall be processed in accordance with the rights of the individual under the Act;
   - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of Personal data and against accidental loss or destruction of, or damage, to Personal data, and;
   - Personal data shall not be transferred to a county or territory outside the European Economic Area, unless that country or territory ensures and adequate level of protection for the rights and freedoms or the individual in relation to the processing of Personal data.

Please contact the University Information Compliance Manager, compliance@lincoln.ac.uk for queries and further information about Data Protection.
6  Internet and Networks

6.1  Introduction

The University promotes and encourages the use of the internet, including Web 2.0 applications such as Facebook, Twitter, YouTube and blogs, as an important means of communication. However, misuse of these facilities can have a negative impact upon the work and reputation of the University.

Users may access internet facilities for the conduct of University related business. The use of the internet is subject to this policy as well as all relevant laws and other University Policies and Regulations.

Users should be aware of the difficulties of taking appropriate care of their own and other peoples Personal or Confidential information when using the Internet. In some situations information may inadvertently or unintentionally become public.

Although most people use the internet for University business, reasonable and sensible personal use of the internet is permitted as long as it does not disrupt or distract the user from the conduct of University business (e.g. due to volume, frequency or time expended) or restrict the use of resources to other legitimate users.

The provision of internet material via computer networks to users is controlled and monitored (as set out in section 9.2) in line with the goals and objectives of the University.

The University internet connection is provided by JANET which connects the UK’s education and research organisations to each other, as well as to the rest of the world through links to the global Internet. JANET and this policy require that users abide by the prevailing JANET Acceptable Use Policy: http://www.ja.net/company/policies/aup.html

6.2  Internet Usage

It is unacceptable to use the University Internet connection or University networks to:

1. View, make, publish or post images, text or materials that are, or might be considered as illegal, paedophilic or defamatory.

2. View, make, publish or post images, text or materials that are, or might be considered as, indecent, obscene, pornographic or of a terrorist nature unless you have a legitimate reason for doing so and have written authorisation from your academic supervisor or head of department.

3. View, make, publish or post images, text or materials that are or might be considered as, discriminatory, offensive, abusive, racist or sexist when the context is a personal attack or might be considered as harassment.
4. View, make, publish or post images, text or material that contravene University Regulations or brings, or may bring, the University into disrepute.

5. Upload, download, link, embed or otherwise transmit commercial software or any copyrighted materials without permission unless this is covered or permitted under a commercial, licence or other such agreement.

6. Download any software, data or other material without implementing effective virus protection measures. The University provides virus protection software to authorised users free of charge (contact the ICT Service Desk on x6500 or helpdesk@lincoln.ac.uk for more information).

7. Intentionally interfere with the normal operation of the network, including the propagation of computer viruses or sustained high volume network traffic that substantially hinders others in their use of the network.

8. Monitor network traffic or contents, or scan devices connected to the network without written authorisation from the Director of ICT Services.

9. Upload to the internet or to unapproved 'cloud' based storage (e.g. Dropbox) Personal or Confidential information without authorisation from your supervisor or line manager AND without ensuring it is strongly encrypted. The University Office 365/One Drive is the only approved cloud storage provision for Personal or Confidential Data. (the ICT Service Desk on x6500 or helpdesk@lincoln.ac.uk can advise on this).
7 Mobiles, Laptops, Tablets and Portable Storage

7.1 Introduction

The University recognises that portable devices play an ever increasing role in day to day business activities. Portable devices require increased levels of awareness because they are so convenient to use.

These devices include laptops, mobile (smart) phones, tablets, iPods, PDAs, memory sticks and cards, CDs, DVDs, Blue-ray disks and other types of storage media available or become available in the future.

Note: University staff using laptops, memory sticks, tablets or other portable media or devices to store Personal or Confidential data (see section 3.1.10 for definition) MUST ensure they are strongly encrypted. See section 7.2.3 below for full details.

7.2 Use of Mobiles, Laptops, Tablets and Portable Storage

1. Under this policy users of ICT Resources must scan any storage device connected to a University ICT resource with virus protection software before or immediately following connection. Users can contact the ICT Service Desk (x6500) for more information about how to do this.

2. Under this policy, users of portable devices (including all the devices mentioned in section 7 introduction) must never, under any circumstances, store or save Credit or Debit card numbers (see section 3.1.9 for definition) on this equipment.

3. The copying of data to portable storage (including all the devices mentioned in section 7 introduction) is governed by different rules according to the sensitivity of the data defined by the UK Data Protection Act (1998), other legislation and government guidelines.

These definitions are:

a. Personal or Confidential data as defined in section 3.1.10.

Data falling into the ‘Personal or Confidential data’ category must never be copied to portable storage under any circumstances except when ALL of the following requirements have been met:

- Copying Personal data has been authorised by the University Information Compliance Manager.

- Copying the data has been authorised by your line or service manager/supervisor.

- It has been encrypted using strong encryption (the ICT Service Desk, x6500, can advise on this)
Data falling into the ‘Other Sensitive Data’ category must never be copied to portable storage under any circumstances except when ALL of the following requirements have been met:

- Copying the data has been authorised by your line or service manager/supervisor.
- It has been encrypted using strong encryption (the ICT Service Desk, x6500, can advise on this).

4. When sending any media or storage device containing sensitive data by post or courier a tracked method must be used, in addition to the requirement to be strongly encrypted. The encryption password must be transmitted to the recipient by an alternative method (e.g. telephone).

5. Email on portable devices, in particular mobile phones is frequently not secure. When accessing University email on portable devices users should ensure that emails and attachments are protected by a password. Emails containing Personal or Confidential data must be encrypted during transmission and storage (see 7.2.3 above). Please contact the ICT Service Desk on x6500 or helpdesk@lincoln.ac.uk for more information.

6. When using offsite printing from portable devices or laptops appropriate care should be taken of information that is Personal Data or confidential information, Please contact the ICT Service Desk on x6500 or helpdesk@lincoln.ac.uk for more information.
8 Remote Access Working

8.1 Introduction

The use of ICT Resources from remote locations has become more practical as technology has advanced. Where appropriate the University seeks to support authorised users when accessing ICT Resources from remote locations.

If ICT Resources are used from a remote location where a stricter security or remote access policy provision applies, the stricter policy provision will apply.

8.2 Remote Access Usage

Under this policy users of ICT Resources must:

1. Ensure they have a legitimate need in terms of University business for remote access working.

2. Obtain proper authorisation from your line or service manager/supervisor for allowing remote access working.

3. Only use the ICT supplied access mechanisms and connection details from ICT Services when remote access working.

4. Agree when using Remote Access using personal equipment (e.g. your own PC) from a remote location, it is used as though it is covered by this policy in all respects.

5. Avoid using remote access working from public systems, such as internet cafes (information, e.g. passwords, might be retained and therefore useable by others).

6. Ensure that when using remote access working - it is not possible for other people to observe the screen.

7. Take appropriate care of Personal or Confidential data by ensuring the data is properly protected in, and to and from, the remote environment. This means encrypting the personal or sensitive data using strong encryption. This could by using a Virtual Private Network (VPN), an encrypted email connection (e.g. https://email.lincoln.ac.uk) and file based encryption. Please contact the ICT Service Desk on x6500 or helpdesk@lincoln.ac.uk for more information.

8. Take appropriate care of Personal or Confidential data by ensuring the data is properly protected when using unsecured wireless connections or unsecured transfer methods (e.g. FTP or unsecured HTTP) in a remote environment. This means encrypting the Personal or Confidential data using strong encryption. This could by using a Virtual Private Network (VPN), an encrypted email connection (e.g. https://email.lincoln.ac.uk) and file based encryption. Please contact the ICT Service Desk on x6500 or helpdesk@lincoln.ac.uk for more information.
9 Compliance

9.1 Applicable Compliance Legislation

The use of University ICT resources is governed by English law.

Some legislation covering use of University ICT resources and this policy is:

- Data Protection Act – 1998
- Computer Misuse Act – 1990
- Copyright, Designs and Patents Act – 1988
- Criminal Justice and Public Order Act – 1994
- Indecent Displays (Control) Act – 1981
- Sexual Offences (Conspiracy and Incitement) Act - 1996
- Telecommunications Act - 1984
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations – 2000
- The Privacy and Electronic Communications Regulations - 2003

This list is not intended to be exhaustive. Details about legislation can be obtained from the Office of Public Sector Information: [http://www.opsi.gov.uk/](http://www.opsi.gov.uk/)

9.2 Email Access, Investigation and Monitoring Provisions

For staff accounts, and because email is provided primarily for business and academic use, it might be necessary to allow another staff member access to an individual user’s accounts for important business purposes (for example, to access time sensitive information when an individual user is on long term absence or is otherwise unavailable). It is recommended that personal emails are clearly marked as such or stored in a personal folder, so that access to them can be avoided should business access be needed. Where possible, an individual’s permission should be sought before allowing access to another staff member.

Normally, ICT infrastructure is only monitored to ensure its efficient and effective operation. This routine performance monitoring does not require content of shared drives or email to be accessed or read, but may involve identifying an ICT user to allow their computer to be fixed or to remove a virus.

However, the University keeps back-ups of information which might subsequently be accessed as part of a properly authorised investigation in accordance with the provisions of English law.

Authorisation for an investigation or monitoring will be sought after a complaint has been received about suspected violations of this or other University policies or regulations or as part of a wider investigation, including allegations of illegal activity.

Examples might include an investigation or monitoring in response to complaints involving cyber bullying or provision of user account information or activity in support of a wider investigation into criminal activity.
Any investigation or monitoring is subject to the following safeguards:

- The investigation or monitoring will be authorised by a senior member of University Staff of at least Pro-Vice Chancellor level;

- The monitoring or investigation will only take place when the authorising senior member of University Staff is satisfied there are grounds for suspecting criminal activity or serious malpractice;

- The investigation or monitoring will be carried out by technically competent staff with appropriate training;

- Records will be kept about what was accessed, when and by whom.

Under normal circumstances the individual(s) concerned will be notified in advance, unless, in the opinion of the authoriser, the notification would make it difficult to prevent or detect wrongdoing.

Statistics and data relating to the use of University ICT resources may be made available to third parties, such as the police, in accordance with English law. This may occur when a lawful request for this information is received or when the University is legally obliged to, or it is appropriate to do so for other reasons.

The University also reserves the right to demand that passwords and decryption keys, where used, be made available, so that it is able to fulfil its right of access to material when a lawful request for this information is received or when the University is legally obliged to.
10 Policy Violations

10.1 Reporting Policy Violations

Violations of this policy can be reported to:

- the ICT Service Desk on x6500 or helpdesk@lincoln.ac.uk;
- abuse@lincoln.ac.uk – particularly for email issues;
- infosec@lincoln.ac.uk – the University Information Security Manager.

If a violation of this policy involves Personal data the University Data Protection Policy requires that the Data Security Breach Management Procedures be followed. Please contact the University Information Compliance Manager:

- compliance@lincoln.ac.uk or x6154.

10.2 Consequences of Policy Violations

Depending upon the circumstance, the consequences of violations of this policy could be any combination of:

1. Access to any or all ICT Resources covered by this policy being denied.

2. Appropriate disciplinary action under the terms of University Regulations or staff contracts of employment.

3. Cancellation of contracts between the University and the user or the organisation that the user works for, or on behalf of.

4. In serious cases, violations of this policy may result in expulsion from the University or termination of a contract of employment.

5. In serious cases of violations of this policy the University or other parties may take civil or criminal action against the user.
11 Relevant Documents

11.1 Other Documents

Other documents that may be relevant to this policy are:

- University Data Protection Policy (internal only)
- University of Lincoln Policy on Intellectual Property Rights - Final
- University of Lincoln web site legal notices
- Web 2.0 Usage Guidelines
- Web Notice and Takedown Policy Guidelines
- Staff Mobile Phone Policy (TBA)

11.2 Document Locations

The current version of this document can be found here:

http://www.lincoln.ac.uk/aup

12 Useful Contacts

12.1 Useful Contacts

If you have any queries about this policy please contact:

- the ICT Service Desk on x6500 (externally: 01522 886500) or helpdesk@lincoln.ac.uk;
- abuse@lincoln.ac.uk – particularly for email issues;
- compliance@lincoln.ac.uk – particularly for data protection issues;
- infosec@lincoln.ac.uk – the University Information Security Manager.
13 Agreement for External Parties

This form is to be signed by external staff, contractors or third-party organisations that are to be allowed to use University of Lincoln ICT facilities.

I/We (delete as appropriate) agree to abide by this University of Lincoln Acceptable Use Policy:

Date ..................................................

Signed for and on behalf of organisation (when applicable):

Full Legal Name: ..........................................................

Address:......................................................................

..................................................................................

Signature: .................................................................

Name:........................................................................

Position:......................................................................

Telephone:...............................................................

Email address:..........................................................