UNIVERSITY OF LINCOLN

ICT Acceptable Use Policy

Quick Summary

1. You must not access any information that you are not permitted to access.

2. You must not use any ICT resource that you are not permitted to use.

3. You must not do anything illegal.

4. You must not create or use offensive material.

5. You must not introduce viruses or do anything else that causes problems for others.

6. Only send personal, confidential and highly confidential data in accordance with ICT's guidelines document on "How to send Personal Data, Special Category Personal Data and Non-Public Information" which is found at the link below.

https://universityoflincoln.sharepoint.com/sites/ICT/InfrastructureServices/ICTPolicies/Document%20Library%202/How%20to%20Send%20Special%20Category%2C%20Personal%20and%20Non-Public%20Data%20v1.0.pdf

7. You could be subject to disciplinary and/or other action if you break the rules.

If you are not sure about anything contact the ICT Service Desk on x6500 or ICT@lincoln.ac.uk.

Author	Dwayne Cassell, Information Security Manager
Approved	D Cook, Director of ICT
Current Version	2.13
Issue Date	14.05.2021
Review Date	05.04.2022

Revision History

Version	Date	Author(s)	Notes on Revisions
1.0	11.09.09	Mark Smith	Version 1 issued.
1.1	15.10.09	Mark Smith	Added unintentional email clause & clarified investigation & monitoring provision.
1.2	30.11.09	Mark Smith, Mike Day	Further investigation and monitoring clarification.
1.3	11.12.09	Mark Smith	Typo and section 4 privacy paragraph.
1.4	10.06.10	Mark Smith	Added PCI-DSS requirements.
1.5	27.07.11	Mark Smith	Data Protection and Mobile improvements
1.51	21.09.11	Mark Smith	Comments from Ann-Marie Noble
1.52	22.09.11	Mark Smith	Further comments from Ann-Marie Noble
1.53	03.10.11	Mark Smith	ICT Security Group Comments
1.54	15.12.11	Mark Smith	Discussions with LH
2.00	11.05.12	Mark Smith	Version 2 issued
2.01	13.06.12	Mark Smith	Added research ethics committee to 4.1.10, corrected section numbers and reissued.
2.02	4.12.13	Mark Smith	New template
2.03	4.12.13	Mark Smith	Minor improvements, PCI-DSS and offsite printing
2.04	18.12.13	Mark Smith	Amended title
2.05	15.07.14	Mark Smith	Added Office 365 as approved cloud provision;
2.06	22.07.14	Mark Smith	Version 2.06 issued
2.07	07.12.15	Drew Cook	Added reference to PREVENT
2.08	28.02.16	Drew Cook	Further revisions following updated PREVENT advice
2.09	17.05.18	Martin Coulson	Removed DPA and added GDPR, Changed 'Confidential' to 'non-public'
2.10	15.08.18	Martin Coulson	Updated to reflect the new information classifications
2.11	17.06.19	Martin Coulson	Minor grammatical changes
2.12	02.07.20	Dwayne Cassell	Updated scope of the document to include applicants. Made conditions of use applicable to all forms of communication and added section of video and collaboration tools. Corrected broken links to other documents, added guidance on sending sensitive and personal data, Best practice guide for Email deliverability, updated contact email addresses for the ICT Service Desk and the Information Security Manager
2.13	06.05.21	Dwayne Cassell	Amended page references under section 8

Approval

This document has been approved by: D Cook – Director of ICT

Signed:	**Date:**

Contents

1 Introduction

1.1 Purpose of Policy

This document defines the University of Lincoln's Information and Communications Systems Acceptable Use Policy (AUP) 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 services.

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 University 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.

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 not to disproportionally 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.

Throughout this document, the term 'Sensitive Data' refers to:

- Personal data (including special category data)
- Confidential data
- Highly Confidential data

Further information on information classification can be found in the UoL's Information Ownership and Classification Policy.

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 when those resources are used;
- 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 which can be contacted on x6500 or ICT@lincoln.ac.uk.

If you feel that your particular requirements for use of ICT resources have not been properly addressed by this policy, then 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 (AUP) 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;
- Applicants applying to 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.

This policy applies to all users of University of Lincoln resources regardless of their role including, but not limited to: support roles, teaching roles, research roles and all students.

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 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, Instagram etc.;
- Application software, services and data including databases;
- Removable media, such as CDs, DVDs and memory sticks;
- Access to resources using personal devices, e.g. devices not provided by the University of Lincoln.

3 General Guidelines

3.1 Principles of this Policy

When using ICT resources and engaging in digital communications such as email, instant messaging and video conferencing, users are expected to comply with the letter and the spirit of this policy and specifically:

1. You must not access any information that you are not permitted to access.

2. You must not use any ICT resource that you are not permitted to use.

3. 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).

4. 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).

5. 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). The University reserves the right to monitor and/or block access to such material.

6. 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).

7. 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.

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

9. You must not send 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.

10. You must not send unsolicited email (‘spam’), chain letters or any form of unauthorised or unsolicited content using University email resources.

11. You must not send 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.

12. You must not compromise or risk compromising the security, confidentiality, availability or integrity of the University's ICT resources in any way whatsoever.

13. 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 spread sheets or other documents, or entered into non approved ICT PCI-DSS systems or devices. If you do receive an email containing a Credit or Debit card number, you must delete it immediately.

14. You must take appropriate care when using sensitive data and abide by all relevant data protection legislation including the General Data Protection Regulation (GDPR).

The ICT guidance on "How to send Personal Data, Special Category Personal Data and Non-Public Information" is found at the link below.

https://universityoflincoln.sharepoint.com/sites/ICT/InfrastructureServices/ICTPolicies/Document%20Library%202/How%20to%20Send%20Special%20Category%2C%20Personal%20and%20Non-Public%20Data%20v1.0.pdf

Also, please refer to the Data Protection Policy below.

https://universityoflincoln.sharepoint.com/sites/SecretariatOffice/IC/Data_Protection/University%20Data%20Protection%20Policy/Data%20Protection%20Policy%20v1.6.pdf

Any staff or students who may be involved in research, professional practice, or other activities that requires them to process, or have access to sensitive 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.

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

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

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

17. You must not use another user's identity or otherwise disguise their, or your own, identity when using any ICT resource. You must only use your assigned account username and password to access University ICT resources; the password must comply with the password policy.

18. You must not use an ICT resource for any unauthorised purpose.

19. 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.

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

21. If you do not consider yourself competent using any ICT resource then you must seek appropriate advice e.g. the ICT Service Desk on x6500 or ICT@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

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.

Staff must only use University email addresses when conducting University business. Emails must not be automatically forwarded from University email addresses to non-University or private email addresses. This is essentially moving the data to an external environment and out of the University's control which presents a potential security risk.

You must not send email to multiple non lincoln.ac.uk email addresses, contained within the same TO or CC fields, without the recorded consent from each of the addressed recipients to share this personal information with the other recipients. BCC must also not be used. Please refer to the guide “Best Practice for Email Deliverability” which can be found at:

https://universityoflincoln.sharepoint.com/sites/ICT/InfrastructureServices/ICTPolicies/Document%20Library%202/Best%20Practice%20for%20Email%20Deliverability.pdf

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).

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, then 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, phishing campaigns 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.

5 Video Conferencing and Collaboration Platforms

Only tools and platforms approved by the University should be used when initiating video conference sessions, online collaboration sessions and similar events.

You should avoid making links providing access to meetings and events publicly available as this may allow uninvited guests to attend.

It is permissible to accept an invitation from a third party using non-approved tools or platforms; however, when taking part in such a meeting you must make sure you are aware of who else is in the meeting and whether the meeting will be recorded.

Some non-approved tools and platforms do not provide an adequate level of protection to ensure security of data and information shared. You must be very aware of any confidential or personal data and information that will be shared during the meeting. You should not share any personal or confidential information during the meeting unless you have received approval to do so by the relevant data owner and if appropriate have a data sharing agreement in place with the respective parties.

6 Software, Services - Applications and Data

6.1 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 must 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 personal information in accordance with the General Data Protection Regulation (GDPR) and all other relevant Data Protection legislation.

6.2 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 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 a software service, application or data requiring proper identification.

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

6. Not to allow sensitive data 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 Service Desk).

   ICT guidance on "How to send Personal Data, Special Category Personal Data and Non-Public Information" is available via the following link:

https://universityoflincoln.sharepoint.com/sites/ICT/InfrastructureServices/ICTPolicies/Document%20Library%202/How%20to%20Send%20Special%20Category%2C%20Personal%20and%20Non-Public%20Data%20v1.0.pdf

7. 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.

8. Not use any designated ICT resource to contravene any aspect of English law.

9. When handling Personal data abide by the General Data Protection Regulation (GDPR) and all other relevant Data Protection legislation.

   Personal data shall be:

   - processed lawfully, fairly and in transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

   - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’)

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’)

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’)

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for the purposes of archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’)

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’)

- the controller shall be responsible for, and be able to demonstrate compliance with, the first principle” (‘accountability’)”

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

7 Internet and Networks

7.1 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 mindful of the inherent risks, associated with exposing their own and other people’s sensitive 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: https://community.jisc.ac.uk/library/janet-services-documentation/janet-policies-and-legal-requirements

7.2 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 contravenes 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 ICT@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) sensitive data without authorisation from your supervisor or line manager

AND without ensuring it is strongly encrypted. The University's Office 365/One Drive is the only approved cloud storage provision for sensitive data. (the ICT Service Desk on x6500 or ICT@lincoln.ac.uk can advise on this).

8 Mobiles, Laptops, Tablets and Portable Storage

8.1 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, Blu-ray disks and other types of storage media available or that may become available in the future.

Note: University staff using laptops, memory sticks, tablets or other portable media or devices to store sensitive data (see section 1.1 for definition) MUST ensure that they are strongly encrypted. See section 8.2.3 below for full details.

8.2 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 8's introduction) must never, under any circumstances, store or save Credit or Debit card numbers (see section 3.1.13 for definition) on this equipment.

3. The copying of data to portable storage (including all the devices mentioned in section 8's introduction) is governed by different rules according to the sensitivity of the data, as defined by the General Data Protection Regulation (GDPR), and other relevant legislation and government guidelines.

   Personal (including special category) data must never be copied to portable storage under any circumstances except when ALL of the following requirements have been met:

   - The copying of the data has been authorised by a University Information Compliance Officer.

   - The copying of 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)

Sensitive data must never be copied to portable storage under any circumstances except when ALL of the following requirements have been met:

- The copying of 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. Email on portable devices, in particular mobile phones, is frequently not secure. When accessing or sending University email from a portable device then users must adhere to the ICT guidelines "How to send Personal Data, Special Category Personal Data and Non-Public Information" available via the following link:

https://universityoflincoln.sharepoint.com/sites/ICT/InfrastructureServices/ICTPolicies/Document%20Library%202/How%20to%20Send%20Special%20Category%2C%20Personal%20and%20Non-Public%20Data%20v1.0.pdf

5. When using offsite printing from portable devices or laptops, appropriate care should be taken of information that is sensitive data. Please contact the ICT Service Desk on x6500 or ICT@lincoln.ac.uk for more information.

9 Remote Access Working

9.1 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.

9.2 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. The ICT Working from Home guidance can be found at https://ict.lincoln.ac.uk/working-from-home/

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 sensitive data by ensuring the data is properly protected in, and to and from, the remote environment. This means encrypting the sensitive data using strong encryption. This could be 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 ICT@lincoln.ac.uk for more information.

8. Take appropriate care of sensitive 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 sensitive data using strong encryption. This could be 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 ICT@lincoln.ac.uk for more information.

10 Compliance

10.1 Applicable Compliance Legislation

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

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

- Data Protection Act 2018
- General Data Protection Regulation (GDPR) - 2016
- Computer Misuse Act – 1990
- Copyright, Designs and Patents Act – 1988
- Criminal Justice and Public Order Act – 1994
- Human Rights Act – 1998
- Indecent Displays (Control) Act – 1981
- Obscene Publications Acts – 1959, 1964
- Regulation of Investigatory Powers Act – 2000
- 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
- The Counter Terrorism and Security Act – 2015

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/

10.2 Email and Internet 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. Access to another person's email must, in the first instance, be authorised by either the person's line manager, or a member of the University's SLT, and where it is possible to do so, the mailbox owner's permission should also be sought.

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.

11 Policy Violations

11.1 Reporting Policy Violations

Violations of this policy can be reported to:

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

If a violation of this policy involves personal data, then the University Data Protection Policy requires that the Data Security Breach Management Procedures be followed.

Contact the University Information Compliance Officers as follows:

Email	compliance@lincoln.ac.uk
Telephone Ext	6618/6184

11.2 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.

12 Relevant Documents

12.1 Other Documents

Other documents that may be relevant to this policy are:

Information security homepage

https://ict.lincoln.ac.uk/infosec

ICT Policies

https://ict.lincoln.ac.uk/infosec/ict-policies/

Data Protection Policy

https://universityoflincoln.sharepoint.com/sites/SecretariatOffice/IC/Data_Protection/University%20Data%20Protection%20Policy/Data%20Protection%20Policy%20v1.6.pdf#search=data%20protection

Intellectual property website

https://universityoflincoln.sharepoint.com/sites/RE/Research%20and%20Industrial%20Partnerships/IP/SitePages/Home.aspx

Website and publications Information liability

https://www.lincoln.ac.uk/home/abouttheuniversity/governance/universitypolicies/websiteandpublicationsinformationliability/

How to send Personal Data, Special Category Personal Data and Non-Public Information

https://universityoflincoln.sharepoint.com/sites/ICT/InfrastructureServices/ICTPolicies/Document%20Library%202/How%20to%20Send%20Special%20Category%2C%20Personal%20and%20Non-Public%20Data%20v1.0.pdf

12.2 Document Locations

The current version of this document can be found here:

https://www.lincoln.ac.uk/home/abouttheuniversity/governance/universitypolicies/informationandcommunicationtechnologyictpol/

13 Useful Contacts

13.1 Useful Contacts

If you have any queries about this policy, please contact:

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

14 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:.…………………………………………..…….…….