Information Security Policy

Document details

Document Reference	Information Security Policy
Document Status	Live
Document Owner	Head of IT Security
Review Period	1 year
Date of First Approval	04/07/2023
Date of Next Review	04/07/2024
Version Number	1.0

Version Control

Version	Date	Description of changes and name and job title of person/body responsible for making changes
0.1	March 2019	Creation of Policy by John Couzins, Head of IT Security
1.0	July 2023	Approved by University Executive Board

Document Governance

The following table identifies who within Lancaster University is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Accountable	Deputy Chief Executive (Operations)
Responsible	Chief Information Officer
Consulted	Digital Strategy Advisory Group, Information Security and Data Governance Sub-Group, InfoSec Policy working group
Informed	All Employees, Temporary Staff, Students, Researchers, Contractors

Table of Contents

1.1. Policy Statement

The Information Security Policy outlines Lancaster University's commitment to maintaining the confidentiality, integrity, and availability of our information and assets. The policy establishes the framework for safeguarding sensitive information, protecting against unauthorised access, and mitigating potential security risks. Adhering to this policy, will enhance the trust of our customers, maintain regulatory compliance, and support the University's strategic goals.

1.2. Purpose

This Information Security Policy provides management direction and support for information security across the organisation. Specific, subsidiary information security policies shall be considered part of this information security policy and shall have equal standing**.**

1.3. Scope

This Information Security Policy applies to all systems, data, people, and processes at the University. This includes but is not limited to all Faculties, Departments, Research Institutes, Professional Service Divisions, Colleges, Staff, Students, Visiting Academics, Teaching Partnerships, Emeritus Professors, third parties and agents of the organisation who have access to IT systems or information used for Lancaster University purposes.

1.4. Definition

This policy shall be applied whenever information, data or information systems are used, shared, or accessed. Information may take many forms and includes, but is not limited to:

- Hard copy data printed or written on paper
- Data stored electronically (on and off premises)
- Communications sent by post / courier or using electronic means
- Stored tape, video or images
- Voice/audio recordings

1.5. Policy Compliance

Any persons found to have breached this policy, may be subject to Lancaster University disciplinary procedures as specified in the People and Organisational Effectiveness (PoE) Disciplinary Procedure and Student Discipline Regulations. If a criminal offence is considered to have been committed, further action shall be taken to assist in the prosecution of the offender(s). Contractors, third parties and all other persons shall be subject to relevant contractual terms and the law.

1.6. Review and Revision

To ensure that the information security policy and associated processes remain fit for purpose, they will be reviewed on the following schedule:

- Review of the Information Security Policy – 1 year (amendments to be approved by Digital Strategy Advisory Group)

- Review of Guidance and Standards 1-2 years (amendments to be approved by representatives under associated responsibilities)

1.7. Accountability

The Deputy Chief Executive (Operations) is accountable for the Information Security Policy and its application at the University. All persons in scope will assist the Deputy Chief Executive (Operations) in the application of this task by ensuring they are aware of their role and responsibilities with respect to information security.

1.8. Responsibilities and Roles

All Persons

- Shall act in accordance with this policy and other associated procedures, standards and guidance established to protect information, and must seek advice and guidance if clarification is required
- Shall ensure that any University issued user identities are not used by any other party(ies) and associated passwords shall not be shared with any other person(s) or other system(s) for any reason
- Shall be aware of the different data classifications and embed a risk-based approach within normal working practices and throughout information handling processes
- Shall report any actual or suspected failure or breach in information security (i.e. any compromise of information confidentiality, integrity, availability or authentication), or working practices which jeopardise the security of the University's information

All Staff

- Shall undertake information security training prior to accessing University data and complete the mandated refresher training, at least every 2 years.

1.9. Groups with special responsibilities:

Data Owners

ANY PERSON CREATING NEW DATASETS OR PERSONS WHO HAVE PRIMARY RESPONSIBILITY FOR ENSURING THE APPROPRIATE USE AND SECURITY OF THE DATA.

Data Owners are accountable for identifying the security classifications for any information assets they create or that are within their area of responsibility as outlined with the University classification scheme to ensure that the appropriate controls, data management policies governing storage, dissemination, disposal and labelling are followed.

The Data Owner is also accountable for ensuring the appropriate technical and organisational measures required to protect the data from loss, destruction or damage are taken. Responsibility for the day-to-day management or administration of systems and processes may be delegated to system owners, but it is the data owner's responsibility to ensure that these responsibilities are carried out.

Systems that store or process data that contains Personal or Special Category data can also be required to undergo a Data Protection Impact Assessment (DPIA). It is the responsibility of the data owner to check if a DPIA is required.

Data Owners shall ensure that Personal data is recorded in the departmental information inventory through their departmental General Data Protection Regulation (GDPR) Representative.

If there is any suspicion that there has been a breach of information security in any of those systems, data owners shall:

- Ensure that any information security incidents are immediately reported.
- Ensure cooperation from all associated parties occurs during the investigation.
- Ensure that changes are made to implement mitigations to avoid reoccurrence.

System Owners

ANY PERSON(S) TASKED WITH ADMINISTERING OR MAINTAINING A SYSTEM OR SERVER

All systems shall have a defined owner or owners. System owners are tasked with the implementation and management of a system as directed by the data owner. The system owner shall configure what information/functions users are permitted to access in line with least privilege principles.

The system owner is responsible for ensuring that users are accessing personal information appropriately for operationally justified reasons as defined by the data owner.

System owners tasked with the technical administration of a server should undertake server administrator training prior to the creation or management of those workloads.

IT Professionals

ANY PERSON(S) WORKING WITHIN INFORMATION SYSTEMS SERVICES (ISS) OR DEPARTMENTALLY BASED STAFF WHO ARE SYSTEMS ADMINISTRATORS FOR ANY INFRASTRUCTURE, SHARED COMPUTER ON THE NETWORK OR APPLICATION DEVELOPERS

IT Professionals shall:

- Utilise their professional knowledge and experience to proactively manage risk while also educating and assisting others in risk management through best practice.
- Always follow change management process when making changes to the way we manage and secure data.
- Respond to potential threats identified through remote scanning of suspect devices, such responses may include removal of those suspect devices from the network.
- Maintain technical controls to ensure the security of the IT infrastructure and systems.
- Escalate issues and concerns in a timely manner to management.

Line Managers

ANY PERSON(S) DIRECTLY RESPONSIBLE FOR MANAGING ANOTHER PERSON OR A TEAM

Line Managers shall:

- Ensure that reportees complete training and are aware of their security responsibilities in accordance with policies and guidelines.
- Ensure that IT assets are handled in line with starting and finishing procedures.

- Respond promptly to any strong indications of staff disaffection that they believe presents genuine risk to University assets, by reporting the disaffection with People and Organisational Effectiveness (PoE), e.g. a genuine statement of intent to compromise information, or an IT assets, confidentiality, integrity or availability.

Strategic Planning and Governance

ANY PERSON(S) WORKING AS PART OF THE STRATEGIC PLANNING AND GOVERNANCE TEAM.

The Information Governance Team within the Division of Strategic Planning and Governance shall provide training and advice to University persons on records management and compliance with information legislation such as the GDPR and the Freedom of Information Act. The Head of Information Governance is also jointly responsible, with the Head of IT Security, and their respective teams for the approval of Data Protection Impact Assessments (DPIAs).

People and Organisational Effectiveness (PoE)

ANY PERSON(S) WORKING AS PART OF THE PEOPLE AND ORGANISATIONAL EFFECTIVENESS (POE) DEPARTMENT.

People and Organisational Effectiveness (PoE) shall ensure that people joining the University or changing role within the University are made aware of their contractual responsibilities when it comes to Information Security.

Emergency Planning & Risk Advisory Group

ANY PERSON(S) WORKING AS PART OF THE EMERGENCY PLANNING & RISK ADVISORY GROUP.

The Emergency Planning & Risk Advisory Group shall review the ongoing development of Operational Risk Management, Business Continuity Management and Emergency Management at the University and ensure training and exercising, including as it relates to information risk, is undertaken within an agreed framework.

Heads of Department / Divisional Directors (or equivalent)

ANY PERSON(S) WORKING IN THE ROLE OF HEAD OF DEPARTMENT, DIVISIONAL DIRECTOR, OR EQUIVALENT ROLE SUCH AS THE HEAD OF AN INSTITUTE OR CENTRE.

The Head of Department / Divisional Director, or any equivalent role, shall ensure that Strategic Planning and Governance are made aware of systems in their department that contain restricted or personal information. They should act as the Data Owner for systems and large data sets that store or collect personal data but may delegate responsibility to a sufficiently senior member of staff within the department.

They are also responsible for ensuring that departmental processes, practices, and research comply with this policy and all other subsidiary policies. They shall ensure that staff and students are aware of their individual responsibilities and obligations, encouraging them to follow the processes and take part in training when appropriate.

Persons Handling or Processing Payments

ANY PERSON(S) PROCESSING OR HANDLING CUSTOMER PAYMENTS

Persons required to handle or process credit card information as part of their role have additional responsibilities as part of the University's compliance with the Payment Card Industry Data Security Standard (PCI DSS). All persons shall ensure they complete the PCI DSS training prior to handling card data and renew the training annually. Persons shall also familiarise themselves with additional policies, specific to payment card handling.

Procurement and persons tasked with purchasing or contractual responsibilities

ANY PERSON(S) REQUIRED TO PURCHASE GOODS AND SERVICES ON BEHALF OF THE UNIVERSITY

Persons who are required to negotiate contracts or purchase goods and services on behalf of the University shall ensure that all purchases and contracts are completed in line with University policies and guidance. They shall ensure that where personal data is required to be shared or accessed by a supplier or third party, GDPR contractual clauses are in place via a data sharing or data processing agreement. These people shall also ensure that personal data is not processed outside of the European Economic Area without additional safeguards in place, as required by the UK GDPR. Further information can be found by contacting the University's Information Governance team.

Facilities personnel and persons responsible for physical access

ANY PERSON(S) TASKED WITH THE RESPONSIBILITY OF ENSURING PHYSICAL SECURITY OF AN ASSET OR SPACE WHICH CONTAINS OR GIVES ACCESS TO ASSETS

Persons employed with responsibilities for ensuring that controls are in place to safeguard physical assets shall do so in line with best practice, adhering to policies and procedures and raising concerns that may negatively impact the confidentiality, availability and integrity of assets in a timely manner.

1.10. Relevant Law

There are a number of laws which relate to use of computer resources; some things which University people may do could not only breach the University's information security policy but may also be illegal. ISS guidance will help University persons comply with this legislation and provide pointers to published material to help give greater detail. ISS will work with People and Organisational Effectiveness (PoE) to offer a programme of workshop events to help spread a greater level of understanding of the relevant legislation.

The Counter Terrorism and Security Act 2015 imposes a duty on Higher Education bodies to engage with the Prevent Duty. This duty requires universities to have 'due regard to the need to prevent people from being drawn into terrorism'. Persons must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. The University reserves the right to block or monitor access to such material.

The relevant law can be found at, for example:

The Copyright, Designs and Patents Act (1988):
https://www.legislation.gov.uk/ukpga/1988/48/contents

Data Protection Act (2018):
https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

The UK General Data Protection Act (2018):
https://www.legislation.gov.uk/eur/2016/679/contents

The Computer Misuse Act (1990):
https://www.legislation.gov.uk/ukpga/1990/18/contents

Prevent Duty Guidance: for higher education institutions in England and Wales (2015)
https://www.gov.uk/government/publications/prevent-duty-guidance/prevent-duty-guidance-for-higher-education-institutions-in-england-and-wales

Regulation of Investigatory Powers Act 2000
https://www.legislation.gov.uk/ukpga/2000/23/contents

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
https://www.legislation.gov.uk/uksi/2000/2699/contents/made

Freedom of Information Act 2000
https://www.legislation.gov.uk/ukpga/2000/36/contents

The Environmental Information Regulations 2004
https://www.legislation.gov.uk/uksi/2004/3391/contents/made

2 Protecting Information

All Persons

2.1. All persons creating new data sets or exporting data sets from existing systems are considered the data owner for that data and accountable for labelling, controlling and disposing of that data in line with data management policies.

2.2. All persons using information systems shall manage the creation, storage, transfer and amendment of data in a manner which safeguards and protects the integrity and security of the data. These people shall also ensure appropriate deletion or destruction of data.

2.3. *Restricted, Personal and Special Category data should only be processed on ISS managed devices or those that have been separately assessed and considered acceptable and in line with minimum device criteria based on risk.

2.4. Restricted, Confidential, Personal and Special Category data shall only be stored or processed on documented systems hosted within the University campus or external systems that have been through the appropriate approval process.

2.5. Restricted, Confidential, Personal and Special Category information shall only be taken for use away from the University in an encrypted form unless its confidentiality can otherwise be assured.

2.6. Restricted, Personal and Special Category data may only be downloaded from University systems where there is an unavoidable business need to do so. Once downloaded it is the individual's responsibility as the data owner that the data shall be held and managed securely, updated appropriately, and deleted immediately when the data is no longer required or in accordance with the University retention policy. Only the bare minimum amount of data required shall be downloaded from University systems.

2.7. *All data sets or systems containing Personal, Special Category or criminal offence data sets shall be recorded in the corresponding departmental information audit register, Data Management Plan or University's Research Ethics system.

2.8. Utmost care will be taken when transporting sensitive data on paper or portable storage media (e.g. disks, CDROMs, laptops and USB flash drives) to keep the media physically secure and under the control of only persons approved to handle the sensitive data.

2.9. Where portable storage media is used, persons in scope shall ensure that valid files are not overwritten, and that incorrect or out-of-date information is not imported from the media. Portable storage media should not normally be used for long term storage of information but where unavoidable, information shall be kept accurate, up-to-date and backed up to a source secured appropriately to the risk.

2.10. *When permanently disposing of equipment containing storage media all sensitive data and licensed software will be irretrievably deleted before the equipment is moved off-site unless done so by a Lancaster University approved contractor.

2.11. Encryption shall be used on all remote access connections to the organisation's network and resources.

2.12. Prior to sending/sharing sensitive information or documents to any persons, not only shall the intended recipient be authorised to receive such information, but the procedures and information security measures adopted by other person(s) shall be seen to continue to assure the confidentiality and integrity of the information.

*Does not apply to third parties or external contractors

2.13. Persons tasked with data input roles shall ensure that data is accurate to the best of their knowledge and adhere to policies, procedures and guidance set out by data owners or system owners.

2.14. Archiving of information and documents shall take place with due consideration for legal, regulatory and operating issues, with liaison between technical and governance staff, and in keeping with the University's retention policy.

2.15. All persons shall be aware of the risk of breaching confidentiality associated with the photocopying (or other duplication) of sensitive documents. Authorisation from the document owner shall be obtained where documents are classified as confidential or higher.

2.16. Hard copies of documents containing personal and/or special category data shall be protected and handled according to the distribution and authorisation levels specified for those documents.

2.17. Hard copies of documents containing personal and/or special category data shall be securely disposed of as soon as they are no longer required.

2.18. *Lancaster University operates a clear desk and screen policy particularly when persons are handling personal data or absent from their normal desk.

2.19. Screens on which confidential or sensitive information is processed or viewed shall be situated in such a way that they cannot be viewed by unauthorised persons. Devices shall be locked when the device's user is no longer physically present at the device.

2.20. The loss, or theft, of any University information asset, classified as confidential or higher, shall be reported via the information security incident reporting form. This would include the loss, or theft, of a non-University device or any portable storage media such as disks, CDROMs, mobile phones, laptops, and USB flash drives that contain University information.

All Staff

2.21. All mobile IT devices and removable storage devices, including those which are privately-owned, that are used to store or access University data shall meet a minimum set of criteria, based on the risk as stated by the University.

Heads of Department / Divisional Directors (or equivalent)

2.22. Each department will maintain an up-to-date and accurate inventory of all Personal Information Assets to which they are considered to be the Data Owner via the departmental information audit register.

Data Owner

2.23. Data owners shall familiarise themselves with any additional contractual or regulatory requirements that relate to the handling and processing of certain datasets and comply accordingly.

2.24. The data owner role shall be transferred to a suitable person for all, non–personally owned, data assets prior to leaving or moving roles within the University.

2.25. The data owner shall ensure suitable backup mechanisms are in place for any data under their ownership.

*Does not apply to third parties or external contractors

2.26. Data stored outside of centrally managed systems shall have a backup mechanism in place appropriate to the data's source and risk associated with its loss. Backup data shall be periodically checked to ensure the backup remains usable.

Data Owners & System Owners

2.27. Personal and Special Category data should be anonymised or pseudonymised wherever practical and only the minimum amount of personal data necessary is to be collected.

IT Professionals

2.28. Any third party used for external disposal of the University's obsolete information-bearing equipment or hardcopy material shall be able to demonstrate compliance with the University's information security policies.

2.29. Standards on security controls should be developed with procedures to provide appropriate levels of protection to sensitive information whilst ensuring compliance with statutory, regulatory and contractual requirements.

Facilities and persons responsible for physical access

2.30. Areas and offices where sensitive or critical information is processed shall be given an appropriate level of physical security and access control.

Line Managers

2.31. Prior to the end of a person's employment or movement to a new position, the role of data owner or systems owner shall be transferred to an appropriate person.

3 Compliance

All Persons

3.1. *University policies and procedures, the student discipline regulations and computer user agreement, set out students' personal responsibilities with respect to the use of computer-based information systems and data. All persons shall comply with this Information Security Policy and, where appropriate, their compliance may be monitored.

All Staff

3.2. The Terms and Conditions of Employment, the Computer User Agreement (CUA) and this information policy set out employees' responsibilities with respect to their use of computer-based information systems and data.

Strategic Planning and Governance

3.3. Before any new systems are introduced which process or store Restricted, Confidential, Personal and Special Category data, a risk assessment process should be carried out which will include an assessment of the legal obligations in relation to information security that may arise from the use of the system. These legal obligations will be documented and a named owner, with responsibility for updating that information, will be identified.

3.4. University Data Retention schedules define the appropriate length of time for different types of information to be held. Data will not be destroyed prior to the expiry of the relevant retention period and will not be retained beyond that period, unless a valid operational reason requires it to be. Any instances where data is required to be retained for longer than the defined retention period should be brought to the attention of the Information Governance Manager. During the retention period appropriate technical systems will be maintained to ensure that the data can be accessed.

3.5. The University will only process personal data in accordance with the requirements of the data protection legislation. Personal or confidential information will only be disclosed or shared once authorisation has been given.

3.6. All University systems will be operated and administered in accordance with the documented procedures. Regular compliance checks should be carried out to verify this compliance.

3.7. Procedures shall be established and widely communicated for the reporting of security incidents and suspected security weaknesses in the organisation's business operations and information processing systems. Mechanisms shall be in place to monitor and learn from those incidents.

IT Professionals

3.8. Guidance shall be made available to all users of systems, informing them of the key aspects related to information security and any associated laws, such as copyright and computer misuse.

*Does not apply to third parties or external contractors

Procurement and persons tasked with purchasing or contractual responsibilities

3.9. All external suppliers contracted to supply services to the University shall agree to follow the Information Security Policies of the organisation. The Information Security Policies should be made available to any such supplier, prior to any supply of services.

3.10. Shall ensure any purchased systems are able to satisfy the requirements set out in our Information Security Policies prior to purchase, such as integrations into our Single Sign-on and geographical data restrictions.

4 Network Access

All Persons

4.1. Password selections, uses, and management must adhere to University standards.

4.2. Shall not share their network connections with third parties and should instead direct them to the appropriate visitor resources.

4.3. Shall not load unapproved software onto ISS-managed PCs, laptops and workstations without explicit consent from ISS.

4.4. All University equipment and those containing data classified as Confidential, Restricted or Personal shall be safeguarded appropriately – especially when left unattended.

4.5. All user-connected devices, or those in the proximity of the Lancaster University network, shall ensure that their connectivity does not negatively affect the confidentiality, integrity or availability, or other systems or data on the network, through secure configuration and guidance in line with the classification of the network and/or data they are accessing.

4.6. All network-connected devices will be subject to continuous monitoring and assessment to ensure that devices are in line with university policies through vulnerability management, security testing and other similar techniques.

4.7. All network-connected devices shall have a registered owner who is accountable for the activity undertaken by that device. Shared use devices require registered owners to take responsibility for ensuring usage is recorded and only permitted by University users unless restrictions are in place on network access.

4.8. All user-connected devices that fail to meet University policy requirements shall be subject to removal at ISS's discretion.

4.9. Data downloaded from the internet, including mobile code and files attached to electronic mail, shall be treated with additional care to safeguard against both malicious code and inappropriate material.

4.10. Only ISS-approved methods of remote network access shall be used to access University IT systems from outside of the campus network.

4.11. The University will monitor all network infrastructure, traffic and connected devices and users to improve service, identify security issues and comply with legal and contractual requirements.

4.12. Shall ensure that ISS authorise the connection of any network devices or network access required by contractors or other third parties they are responsible for.

5 Agile Working and Mobile Computing

All Persons

5.1. *Users working remotely shall familiarise themselves with the advice and guidance provided by the University.

5.2. IT assets connected to Lancaster University internal networks via remote network access technologies shall ensure that sessions are disconnected when not in use and that other users are not able to gain access.

5.3. All mobile devices used to access or store University personal information shall be subject to the same measures of protection that are set based on asset classification and risk (such as encryption, patching and management) to reduce opportunities for loss or compromise of the information.

5.4. IT assets connected to Lancaster University internal networks, via remote network access technologies, shall be subject to the same policies as devices physically connected to the campus infrastructure.

All Staff

5.5. Users should not create or store sensitive data on personally owned devices, this includes the use of file synchronisation tools. Non-classified information should not be stored on the device unless a copy is also stored in a University owned system.

5.6. Users shall ensure that any IT asset (including smartphones) used to work on University information remotely have been secured according to the relevant provisions of the University's encryption requirements, use up-to-date antivirus software (where supported), are protected by a sufficient password/pin, are in line with the University patching policy and are securely wiped prior to disposal via a method appropriate to the source and risk associated with loss of the device or its stored data.

5.7. All remote working agreements shall include appropriate measures, based on a risk assessment, to protect the security of information assets. Remote workers shall follow the agreed security procedures at all times.

5.8. All remote working agreements shall include rules on the use of equipment provided for teleworking. Teleworkers shall abide by these rules at all times unless specifically authorised.

*Does not apply to third parties or external contractors

6 Collaboration

All Persons

6.1. *Collaboration and file sharing services not provided on behalf of the University shall not be used to store Confidential, Personal or Special Category Information unless the Data Owner has obtained formal approval from the University Information Governance Manager and Head of IT security.

6.2. Users shall be responsible for the appropriateness of sharing data from University approved systems with other services and where appropriate should prepare a data sharing agreement or equivalent document.

6.3. Collaboration services provided on behalf of the University shall be linked to the user for security and audit purposes.

6.4. *Lancaster University reserves the right to reallocate access to data assets where an appropriate reason exists, and a request has been raised through appropriate approval channels.

6.5. Users shall treat information received via email with care due to its inherent information security risks. File attachments should be scanned for possible viruses or other malicious code.

6.6. Email should not be used to communicate Confidential, Personal or Special Category information unless appropriate measures (e.g. encryption) have been taken to ensure authenticity and confidentiality, that it is correctly addressed and that the recipients are authorised to receive it.

6.7. Email addresses shall be checked carefully prior to dispatch, especially where the information content is sensitive; and where the disclosure of email addresses or other contact information to the recipients is a possibility.

6.8. *All email shall be subject to automated scanning for malware, phishing, spam. All email is subject to transaction logging.

6.9. An individual's University email account should not be used for the regular dissemination of large-scale mailshots, research, surveys, or notification. Such email use may break contractual terms or fall under data protection legislation and the sender shall ensure adherence to relevant law and policy.

All Staff

6.10. Whilst the University accepts moderate and reasonable personal usage, email should be used for business purposes in a way which is consistent with other forms of business communication.

6.11. University email accounts shall not be configured to automatically forward email to external email service providers.

6.12. Persons manually forwarding mail shall do so only after verifying that the content is appropriate for the desired audience.

6.13. The attachment of data files to an email shall only be permitted after confirming the classification of the information being sent.

6.14. University staff are responsible for the archiving of material in email accounts in line with the appropriate retention policies.

*Does not apply to third parties or external contractors

6.15. Staff sharing data with guest users via collaboration services shall ensure the appropriateness of the data being shared

6.16. Staff shall not use unapproved third-party email or collaboration systems such as Google, Dropbox and Hotmail to conduct University business, to create or memorialise any binding transactions, or to store or retain email or data on behalf of the University. Research collaboration with institutions that do not use an approved system is only allowed in circumstances where no other approved system, common to both groups, could be used instead. In such situations the data will remain exclusively within the other institutions systems and ownership.

System Owners

6.17. Systems generating emails shall abide by University security policies and follow technical implementation guidelines. System owners are responsible for ensuring the systems meet data protection policy and comply with the law. System owners should provide guidance to users on sharing of data using collaboration services or email from their system.

7 Outsourcing and Third Party Access

All Persons

7.1. *The use of non-University approved cloud services for the storage of any University business data or any data classified as Personal, shall not be permitted without formal approval from ISS or Strategic Planning and Governance.

7.2. Users sharing data with third parties are ultimately responsible for their actions and should take appropriate measures to ensure they understand the risks and policies applicable.

7.3. All third parties who are given access to Lancaster University's information systems, whether suppliers, customers or otherwise, shall agree to follow Lancaster University's Information Security policies.

7.4. Information Security Policies and the third party's role in ensuring compliance should be made available to any such third party, prior to them being granted access.

All Staff

7.5. When sharing sensitive data with non-university members, ensure this is done in line with the University's guidelines via a method that is appropriate to the risk of its associated loss.

7.6. Where personal data is required to be shared with a supplier or third party the Information Governance manager should be consulted and will advise on whether the GDPR data processor clauses require signing or whether an information sharing agreement needs to be put in place.

Strategic Planning and Governance & IT Professionals

7.7. The organisation will assess the risk to its information. Where deemed appropriate because of the confidentiality, sensitivity or value of the information being disclosed or made accessible, the Information Governance manager and Head of IT Security will determine if a DPIA is required to be completed.

Strategic Planning and Governance

7.8. Any facilities management, outsourcing or similar company with which this organisation may do business should be able to demonstrate compliance with the information security policies and enter into binding service level agreements that specify the performance to be delivered and the remedies available in case of non-compliance.

Procurement and users tasked with purchasing or contractual responsibilities

7.9. All contracts with external suppliers for the supply of services to the organisation shall be monitored and reviewed to ensure that information security requirements are being satisfied. Contracts shall include appropriated provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier.

7.10. Persons responsible for agreeing maintenance and support shall ensure that the contracts being signed are in accordance with the Information Security Policies, and compliant with any applicable legislation, e.g. GDPR, Data Protection Act 2018, etc.

*Does not apply to third parties or external contractors

8 Asset Management

All Persons

8.1. *Any lost or stolen University IT asset shall be immediately reported to the Security Operations Manager. The Head of Procurement should also be informed so that an insurance claim can be made where appropriate.

8.2. *The transferring of IT assets to another asset owner shall only take place once approved by the appropriate authority and after it has been recorded in central asset systems. This includes the return of the IT asset to an appropriate IT professional to ensure it can be securely wiped of data before the transfer.

8.3. On cessation of employment, or at the end of contract, all University IT assets including laptops, tablets and mobile phones shall be returned to ISS for re-use, recycling, or disposal in line with the Waste Electric and Electronic Equipment (WEEE) Regulations, this includes equipment funded through research grants or other external sources.

8.4. *All University IT assets shall be centrally recorded into a single asset register unless explicit approval for an exception is given by the Head of IT Security.

8.5. Any software installed on University assets shall be legitimately obtained or purchased and be available for licence audit if required.

8.6. Shall comply with the terms outlined in any software licence and user agreements upon cessation of employment, or at the end of contract, to remove any software that was licensed during affiliation with Lancaster University.

8.7. *Installation of software on specific platforms shall be done in line with agreed standards when installed on University assets or involving University licensed software.

8.8. University owned IT assets shall run centralised asset management software ensuring no local changes to the agent software may occur. Exceptions to this are only allowed with either explicit approval from the IT security team or where a device is unsupported by the asset software, and so will not function correctly.

IT Professionals

8.9. All hardware assets shall be tagged and recorded with an asset owner in centralised asset management software prior to deployment.

8.10. All hardware assets shall be recorded and disposed of in line with associated procedures.

8.11. Assets used for accessing or storing sensitive data should be labelled or identifiable according to sensitivity.

Procurement and users tasked with purchasing or contractual responsibilities

8.12. Procurement of software and cloud services shall be centrally procured unless prior agreement is already in place with procurement or the Software Licence Management team.

8.13. Procurement of IT assets which connect to or permit connections onto the University network shall be restricted to named individuals or when explicit approval has been granted by those individuals.

*Does not apply to third parties or external contractors

9 People Policy

All Persons

9.1. *Any information security incidents resulting from non-compliance may result in appropriate disciplinary action, in line with the People and Organisational Effectiveness (PoE) Staff Disciplinary Procedure or Student Discipline Regulations.

All Staff

9.2. Shall comply with the Information Security policies of the University.

9.3. Access to systems and facilities are provided for business purposes only, whilst the University accepts moderate and reasonable personal usage all communications using a University account or infrastructure are done so under the association of the University. Lancaster University therefore reserves the right to access, read, and store a user's information when there is a business justification and appropriate multi-department approval process.

9.4. Staff shall not remove any data classified as Restricted, Confidential, Personal and Special Category, obtained in the course of their duties at the University when they leave University employment.

9.5. All staff who have access to staff or student personal data shall also be required to complete refresher training at least every two years. The Information Governance team monitors induction and refresher training compliance.

People and Organisational Effectiveness

9.6. All new staff shall receive mandatory information security awareness training as part of induction. Departing staff should be treated fairly and informed, particularly with regard to the termination of their access privileges.

9.7. An appropriate summary of the information security policies shall be made available to, and accepted by, all temporary staff prior to their starting any work for the organisation.

9.8. All employees shall sign a formal undertaking concerning the need to protect the confidentiality of information both during and following their employment with the organisation.

9.9. The organisation is committed to providing training to all users of new systems to ensure that their use is both efficient and does not compromise information security.

9.10. Access privileges should normally be removed on the last contractual day. No further access will be allowed unless another relationship is established between the University and the departing member of staff, e.g. emeritus status.

9.11. Employees agree to abide by the organisations information security policies, and new employee references shall be verified appropriately.

9.12. Shall ensure contract dates are present and correct for all staff members ensuring staff access to systems is appropriately provisioned and deprovisioned in line with timings in contractual agreements.

9.13. Shall assess situations, such as any strong indication of staff disaffection, which may impact information security raised by persons, and inform the Information Security team via appropriate channels.

*Does not apply to third parties or external contractors

9.14. The Terms and Conditions of employment of the University shall include requirements to comply with information security policies.

Heads of Department / Divisional Directors (or equivalent)

9.15. Where staff change jobs, their information security needs shall be reassessed, and any new training provided as a priority. Where staff move roles within the University, it is the responsibility of the Head of Department, Divisional Director (or equivalent), to ensure processes exist for line managers to follow, to ensure that their access privileges are removed or modified appropriately.

Line Managers

9.16. Shall respond promptly to any strong indications of staff disaffection that they believe present a genuine risk to University assets, such as a genuine statement of intent to impact the confidentiality, integrity or availability of information, or an IT asset. In such instances line managers shall liaise with, and report to, Head of Department / Divisional Director (or equivalent), the Head of IT Security and People and Organisational Effectiveness as appropriate.

9.17. Shall ensure reportees complete training and are aware of their security responsibilities in accordance with policies and guidelines.

9.18. Shall ensure that IT assets are handled in line with starting and finishing procedures. They shall ensure all departing staff return all IT assets and access tokens belonging to the organisation. This includes the return of an IT asset to an appropriate IT professional to ensure it can be securely wiped of data before transfer to another person, or securely disposed of when no longer required.

Heads of Department / Divisional Directors (or equivalent) & People and Organisational Effectiveness

9.19. Upon notification of a staff resignation, the Head of Department / Divisional Director (or equivalent), and People and Organisational Effectiveness management shall consider whether the member of staff's continued system access rights constitutes an unacceptable risk to the organisation and, if so, revoke all access rights immediately.

IT Professionals

9.20. Training in information security threats and safeguards should be completed by technical staff, the training should be both appropriate to the role and the risk that is posed to the University.

10 Emergency Planning and Business Continuity Management

All Staff

10.1. All staff shall be made aware of the University Emergency Planning & Business Continuity framework, and their own respective roles within the framework and the University Emergency Management Plan.

Heads of Department / Divisional Directors (or equivalent)

10.2. Management shall develop emergency plans and business continuity plans which cover all business activities in line with University requirements.

10.3. Each emergency plan, contingency plan and business continuity plan will be reviewed bi-annually or when deemed appropriate post incident/significant change.

Emergency Planning & Risk Advisory Group

10.4. Management review potential risks to determine the requirements of a contingency plan or a business continuity plan.

10.5. The organisation will identify a structure for emergency management, business continuity and incident response with inbuilt reviews post incident to identify appropriate areas for further action.

10.6. A formal risk assessment exercise will be conducted to classify systems according to their level of criticality to the organisation and to determine where emergency planning is needed.

10.7. A suite of contingency plans will be available for identified scenarios that should be utilised in the event of an incident impacting information security.

10.8. Plans will be periodically tested. The frequency of testing will be as defined for the appropriate criticality level and will include tests to verify whether management and staff are able to put the plan into operation.

11 System Management

Data Owners

11.1. Systems used for core University business, including those processing Personal or Special Category data, shall be managed by suitably trained, or qualified, staff to oversee their day-to-day running and to preserve security and integrity.

11.2. Procedures shall be established for information systems to ensure that user access rights are managed in line with least privilege principles, in a timely manner, whenever there is a change in business need or staff role. Users' access rights shall be reviewed at regular intervals.

11.3. New IT systems that intend to store or process Personal or Special Category data shall be made aware to the Information Governance Manager and Head of IT Security to determine whether a DPIA is required prior to the collection or transfer of data.

11.4. Procedures shall be established for ensuring that ongoing risk management and compliance adequacy checks take place for all cloud services.

Data Owners & System Owners

11.5. Prior to approval, all new or significant upgrades to systems shall be tested to ensure that they comply with the organisation's information security policies, access control standards and where applicable, still adhere to the principals set out in the initial DPIA or data processing agreement.

11.6. Use of the central authentication service specified by ISS shall be used when deploying new systems as its primary method. Systems unable to comply with this requirement should be able to provide appropriate measures and assurances around account management and be approved by the relevant HoD or business risk owner.

11.7. User access granted to all systems shall be authorised by the manager, delegated authority responsible for the system or the responsible user on multi-user systems. A record shall be maintained of such authorisations, according to the risk level, including the appropriate access rights or privileges granted.

11.8. Access controls shall be maintained at appropriate levels for all systems by ongoing proactive management and any changes of access permissions shall be authorised by the manager of the system or application. A record of access permissions granted shall also be maintained.

11.9. All systems that store, transmit or grant access to data classified as Confidential, Personal or Special Category data should perform suitable logging according to the risk of the asset. Logs should be reviewed periodically.

12 Infrastructure Management

IT Professionals

12.1. Access to the resources on the network shall be strictly controlled to prevent unauthorised access and access control procedures shall provide adequate safeguards through robust identification and authentication techniques. Access to all computing, information systems and peripherals shall be restricted unless explicitly authorised.

12.2. The organisation's network shall be managed by suitably authorised and qualified staff to oversee its day to day running and to preserve its security and integrity in collaboration with individual system owners.

12.3. Networks and communication systems shall all be adequately configured and safeguarded against attacks that impact confidentiality, integrity, and availability.

12.4. Procedures for the registration and deregistration of users and for managing access to all information systems shall be established to ensure that all users access rights match their authorisations. These procedures shall be implemented only by suitably trained and authorised staff.

12.5. The network shall be segregated into separate logical domains with routing and access controls operating between the domains. Appropriately configured firewalls shall be used to protect the networks supporting the organisation's business systems.

12.6. Devices shall be placed on appropriate networks based on the functionality of the device, its level of trust or the responsible person who it is registered to.

12.7. Remote access to the network will be subject to robust authentication and may be limited based on the location, ownership or capability of the device accessing the network. Encrypted communication channels shall be used to access networks remotely.

12.8. Access controls for all information and information systems shall be set at appropriate levels in accordance with the value and classification of the information assets being protected.

12.9. Development of code that may impact, or that is for or to be deployed to, business-critical systems shall incorporate secure coding practices. This is to ensure the avoidance of common coding vulnerabilities and allow resilience against high-risk threats, before being deployed in production.

12.10. Development and testing facilities for business-critical systems should be separated from operational facilities and use pseudonymised or dummy data.

12.11. The implementation of new or upgraded software shall be carefully planned and managed. Formal change control and approval procedures, with audit trails, shall be used for all changes to systems. All changes shall be properly tested and authorised before moving to the live environment.

12.12. Modifications to underlying code or modifications not supported by the vendor shall be discouraged, only strictly controlled essential changes shall be permitted and the development of interfacing software shall only be undertaken in a planned and controlled manner.

12.13. Capacity demands of systems supporting business processes shall be monitored. Projections shall be created of future capacity requirements and used to ensure adequate processing power, storage and network capacity is available in the future.

12.14. The network shall be designed and configured to deliver high performance and reliability to meet the organisation's needs whilst providing a high degree of access control and a range of privilege restrictions.
12.15. The implementation of new or upgraded software, configurations or firmware shall be carefully planned and managed. Formal change control procedures shall be applied to all University business systems, with audit trails, and shall be used for all changes to critical systems or network components. All changes shall be properly tested and authorised before moving to the live environment.
12.16. Equipment supporting core business systems shall be planned to ensure that adequate processing power, storage and network capacity are available for current and projected needs, all with appropriate levels of resilience and fault tolerance. Equipment shall be correctly maintained.
12.17. Equipment supporting business systems shall be given adequate protection from environmental hazards and failures of electrical power or other utilities.
12.18. All University systems and data shall have a backup mechanism, or system, in place appropriate to the source and risk associated with its loss. Backups will be checked periodically to ensure they remain usable. Backup systems shall have a named, accountable, IT professional assigned to them.
12.19. Security technologies, such as anti-malware and intrusion detection systems shall be deployed to assets and infrastructure, ensuring they are up-to-date and configured to block or quarantine identified issues and report them back centrally.
12.20. System date and time shall be regularly synchronised using the University central time systems.

Facilities and persons responsible for physical access

12.21. Networks and communication systems shall all be adequately safeguarded against both physical attack and unauthorised intrusion.