Document Details

Document Reference	**Data Protection Policy**
Document status	**Live**
Document owner	Information Governance Manager
Review period	2 years
Date of first approval	2019
Date of next review	2025
Version number	1.3

Version control

Version	Date	Description of changes and name and job title of person responsible for making changes.
0.1	May 2018	Creation of Policy by Information Governance Manager.
0.2	June 2018	Addition of 'Responsibilities' section Information Governance Manager.
0.3	August 2018	Addition of 'GDPR Representatives' section Information Governance Manager.
0.4	August 2018	Creation of Key Performance Indicators. Information Governance Manager.
0.5	November 2018	Consultation from PwC. Minor changes to wording within 'Responsibilities' and 'GDPR Principles' sections, Information Governance Manager.
0.6	December 2018	Changed responsibilities for IT Security Manager. Information Governance Manager.
1.0	February 2019	Policy approved by Vice-Chancellor.
1.1	April 2019	Updated some broken hyperlinks. Information Governance Manager.
1.2	March 2021	Review of Policy. Updating of URL links. Removal of references to Box. Updated job titles where appropriate. Information Governance Manager.
1.3	January 2023	Updated job titles and links. Added reporting to Information Security & Data Management sub-committee, UEB and Audit Committee. Added new Records Management Officer role. Added in section concerning DLP.

Referenced policies and documents

Information Security Policy Data Security Breach Procedure

Policy on Categorising and Protecting University Information Assets

Risk Management Policy

Data Protection Policy

1. Introduction

1.1 Lancaster University undertakes to comply with applicable data protection legislation as part of its everyday working responsibilities. Lancaster University is fully committed to full compliance with the requirements of the General Data Protection Regulation (UK) and the Data Protection Act 2018.

1.2 The University will ensure that all staff, students, volunteers, and contractors who have access to personal data held by the University are made fully aware and trained on their responsibilities under data protection legislation.

2. Purpose

2.1 The purpose of this document is to define the Data Protection Policy for Lancaster University and to ensure the University's compliance with the UK General Data Protection Regulation (UK)(GDPR) and the Data Protection Act 2018. This Policy should be read in line conjunction with the Lancaster University Information Security Policy.

2.2 The University is committed to ensuring compliance with relevant data protection laws and will:

- have processes in place to ensure that the rights of data subjects, as defined under data protection legislation, are appropriately honoured;
- implement processes and policies to ensure that the data protection principles are adhered to when processing personal or special category information;
- ensure that the University is sufficiently accountable for its information processing activities, as described within Articles 5 and 24 of the UK GDPR;
- ensure that records of all processing activities are maintained and regularly reviewed; and
- ensure that all information processing activities have an appropriate legal basis.

3. Scope

3.1 This Policy is applicable to all staff at the University, including temporary, casual, and agency staff, and volunteers and contractors where acting on behalf of the University. It also applies to third party organisations who may hold information, subject to the UK GDPR or the Data Protection Act 2018, on behalf of the University.

3.2 The Policy applies to students where they are processing personal data on behalf of the University but not where they are processing personal data for non-University or private purposes.

4. Definitions

4.1 *Personal information*

Data which includes information relating to a living person who can be identified or who is identifiable, directly from the data in question, or who can be indirectly identified from that information in combination with other information.

4.2 *Special Category information*

Personal information, which the UK GDPR states is more sensitive, and requires more protection. A full list of special category data items is available from the Information Commissioner's Office website.

4.3 *Information Commissioner's Office (ICO)*

The ICO is the data protection supervisory authority for the UK. The ICO has specific responsibilities set out in both the UK General Data Protection Regulation and the Data Protection Act 2018. The ICO has a range of powers where they believe organisations are not meeting their statutory requirements, ranging from criminal prosecution, the imposition of monetary penalties on organisations and the power of audit.

4.4 *Data Controller*

A data controller is the organisation that determines the purposes and means of processing of personal information.

4.5 *Data Processor*

A data processor is anyone (other than an employee of the data controller) who processes data on behalf of the data controller.

4.6 *Anonymisation*

Anonymisation is the process of turning personal information into a form which does not identify individuals and where identification is not likely to take place. This allows for much wider use of the information.

4.7 *Pseudonymisation*

Pseudonymisation is a process where information is replaced with a pseudonym, e.g. names replaced with numbers. Pseudonymisation only provides limited protection of identity of data subjects and there is often a 'key', which will allow re-identification of individuals.

4.8 *Data Loss Prevention*

Data Loss Prevention (DLP) is an umbrella term used for the approach and implementation of procedures and/or tools used to control the flow of data. The ultimate purpose of implementing DLP is to safeguard data and ensuring it is handled correctly by authorised parties. In order to safeguard data, including personal data within the scope of UK data protection legislation and this Policy, the University will put a DLP Strategy in place.

5. Responsibilities

5.1 *Vice-Chancellor*

The Vice-Chancellor of Lancaster University has overall responsibility for the strategic and operational management of the University and ensuring that the University policies comply with all legal, statutory and good practice guidance requirements.

5.2 *Deputy Chief Executive (Operations) and Secretary*

The Deputy Chief Executive (Operations) (DCE) has overall responsibility for professional services and the operation of governance at the University. The DCE will be the first point of escalation for any issues that require senior management input. The DCE will report to the Vice-Chancellor where appropriate, such as where a data security breach requires consideration for reporting to the data protection regulator.

5.3 *Director of Strategic Planning and Deputy Secretary*

The Director of Strategic Planning and Deputy Secretary has delegated responsibility for ensuring effective implementation and monitoring of this policy. In addition, the Director of Strategic Planning and Deputy Secretary will provide advice to the Vice-Chancellor in regard to any information risk and will provide assurances with regards to compliance with this policy. The Director of Strategic Planning and Deputy Secretary will report to the University DCE.

5.4 *Head of Governance Services*

The Head of Governance Services will line manage the Information Governance Manager and provide operational support and guidance to the Information Governance team. The Head of Governance Services will report to the Director of Strategic Planning and Deputy Secretary.

5.5 *Information Governance Manager*

The Information Governance Manager is the nominated Data Protection Officer for the University; please refer to section 6.10 of this policy for an explanation of the duties of this role. The Information Governance Manager will be responsible for:

- day-to-day responsibility for monitoring compliance with this policy by all areas of the University;
- maintaining the appropriate data protection registrations with the Information Commissioner's Office;
- ensuring that the University's suite of Privacy Notices are kept accurate and up-to-date;
- advising staff on any data protection issues which may arise at the University;
- maintaining a suite of policies and standard operating procedures to ensure the University is compliant with appropriate data protection legislation;
- logging and investigating personal data security breaches which are reported to the Information Governance Team. More information on how the University manages personal data security breaches can be found in section 6.8 of this policy;
- provide monthly compliance reports to the Information Security and Data Management (IS&DM) Sub-Committee including reporting on the KPIs identified in this Policy and any other data protection or information rights issues;
- provide annual compliance reports to the University Executive Board and Audit Committee;
- advising on the strategic direction of the data protection agenda at the University; and
- monitoring compliance and reviewing the success of University, Induction and Refresher, Information Security training and awareness raising activities.

The Information Governance Manager will report to the Head of Governance Services and the Director of Strategic Planning and Deputy Secretary.

5.6 *Information Governance Officer(s)*

The Information Governance Officer(s) will support the Information Governance Manager in fulfilling their responsibilities, as outlined in this policy. The Information Governance Officer(s) will have responsibility for answering any data protection queries from staff and escalating critical queries and incidents/near misses to the Information Governance Manager. The Information Governance Officer(s) will be responsible for compiling reports against Key Performance Indicators, as explained in section 6.12 of this policy.

5.7 *Head of IT Security*

The Head of IT Security is responsible for the day-to-day monitoring of the University's computers, networks and data, to protect against threats such as security breaches, computer viruses, attacks by cyber criminals and credit/debit card fraud. It is the responsibility of individual systems owners to work to recommended standards, carrying out Data Protection Impact Assessments where appropriate, and to respond to concerns identified by the Head of IT Security.

The Head of IT Security will be responsible for assisting the Information Governance Team in investigating reported personal data security breaches, in line with the University's 'Data Security Breach Procedure'.

The Head of IT Security will be responsible for authoring the University's Data Loss Prevention Strategy, supported by the Information Governance Manager and Records Management Officer.

The Head of IT Security will work with the Information Governance Manager and the Digital Fluency Manager to regularly review and update relevant sections of the University's Information Security Training and associated awareness raising campaigns. The Head of IT Security reports to the Head of the Technical Infrastructure Group.

The IT Security Manager will work with the Information Governance Manager to regularly review and update the University Information Security Policies.

5.8 *Records Management Officer*

The Records Management Officer will be responsible for supporting the Information Governance Manager to develop and enhance the University's records management culture and practice, ensure records retention schedules are in place and adhered to support compliance with appropriate legislation and ensure that efficient and effective business processes are in place. Other responsibilities of the Records Management Officer will include:

- being the subject matter expert for all matters concerning records management and retention;
- producing and promoting effective records management policies, procedures and guidance;
- carrying out Department/Division/Faculty records management audits and providing audit outcomes recommendations; and,
- creating, maintaining and delivering records management training to University staff.

5.9 *All University Staff, Volunteers & Governors*

All University staff, including temporary, casual and agency staff and, volunteers and Governors have a responsibility for compliance with this policy. All staff are responsible for being aware of the information governance requirements of the University, including the need to maintain the confidentiality and security of personal information and the requirement to report any breaches of this policy or any applicable data protection legislation.

5.10 *Students*

This Policy applies to students where they are collecting personal information on behalf of the University. For example, conducting research on behalf of the University, collecting personal data as part of their role as a student ambassador or Assistant Dean.

Students who are collecting personal data for their own purposes are not subject to this Policy, but would still be expected to comply with their legal obligations under the General Data Protection Regulation, Data Protection Act 2018 and the Common Law Duty of Confidentiality.

6. Data Protection Policy

6.1 *Data Protection Principles*

Lancaster University is required to comply with the six principles of data protection contained within Article 5 of the GDPR. These principles share similarities with the eight principles contained within the Data Protection Act 1998. The six principles of GDPR are:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. 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 not be considered to be incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (also known as *'data minimisation'*);
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. 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 archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. 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.

Article 5(2) of the GDPR also requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles".

Non-compliance with GDPR can result in a monetary penalty notice being issued by the Information Commissioner's Office, the data protection regulatory body. Monetary penalties under GDPR can reach up to £17.5 million or 4% of global turnover, whichever is greater.

In order to demonstrate compliance the University will maintain records of all processing activities it undertakes. The Information Governance team will retain these records.

6.2 *Lawful basis for processing*

In order to process personal information the University must meet one of the legal basis contained within Article 6(1) of the GDPR. In order to process special category personal information the University must also meet one of the legal basis contained within Article 9(2).

The legal basis for processing must be determined before the processing commences and should be recorded within the University's suite of Privacy Notices.

For the processing of personal data to be legal under GDPR the University must determine which legal basis the data is being processed under. There are six legal basis listed in Article 6(1) of the GDPR.

(a) **Consent**: the data subject has given clear consent for you to process their personal data for a specific purpose.

(b) **Contract**: the processing is necessary for a contract you have with the data subject, or because they have asked you to take specific steps before entering into a contract.

(c) **Legal Obligation**: the processing is necessary for you to comply with the law.

(d) **Vital Interests**: the processing is necessary to protect someone's life.

(e) **Public Task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) **Legitimate Interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is good reason to protect the data subject's personal data which overrides those legitimate interests.

Consent is not the only legal basis for processing someone's personal data. In fact, the majority of the University's core activities are covered under Public Task legal basis rather than consent. The Public Task legal basis can be used for the majority of the University's core activities.

If it is decided that consent is the appropriate legal basis for the processing of personal information, this will affect data subject's rights. Generally, when relying on consent as a legal basis the data subject would have stronger rights than if one of the other legal bases were utilised, such as the right to erasure and the right to data portability.

For further information regarding data subject's rights, please follow this link or contact the Information Governance Manager by emailing: information-governance@lancaster.ac.uk

6.3 *Lawful basis for processing special category data*

For the processing of special category data to be legal under GDPR **two lawful bases** of the GDPR must be met. One of the lawful bases from the six listed in Article 6(1) must be met, and one of the ten lawful bases listed in Article 9(2) must also be met.

The choice of legal basis under Article 6(1) does not necessarily dictate which lawful basis under Article 9(2) is most appropriate. For example, using **Consent** under Article 6(1) does not mean that 'Explicit Consent' under Article 9(2) must be chosen.

The ten lawful bases for processing special category data listed in Article 9(2) are as follows.

(a) **Explicit Consent**: the data subject has given explicit consent to the processing of special category data for one or more specified purposes.

(b) **Obligations and Rights**: processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

(c) **Vital Interests of the data subject or another person**: processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

(d) **Legitimate Activities**: processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

(e) **Public Domain**: processing relates to personal data which are manifestly made public by the data subject.

(f) **Legal Claims**: processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

(g) **Substantial Public Interest**: processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

(h) **Health and Social Care**: processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.

(i) **Public Health**: processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

(j) **Archiving/Research**: processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

6.4 *Privacy Notices/Fair Processing Notices*

In order to comply with GDPR and national data protection legislation the University is required to inform data subjects of how their data will be processed. Privacy Notices/Fair Processing Notices were previously required under the Data Protection Act 1998, under GDPR however the Privacy Notice is required to be more detailed. The GDPR states that data controllers must create Privacy Notices that are:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge

Lancaster University has developed a suite of Privacy Notices, which cover the University's processing activities. These are available from the University website here.

6.5 *Information Security*

All University staff are responsible for ensuring the security of information that they process as part of their role at the University. Staff must ensure that personal information is not disclosed to any unauthorised third party. All staff must appraise themselves of the University's Information Security Policy and the Policy on Categorising and Protecting University Information Assets.

All new staff are required to complete the University's 'Information Security' online e-learning module, within 6 weeks of the commencement of their employment. This e-learning module includes training on data protection for University staff.

6.6 *Refresher Training*

University staff who routinely have access to personal and/or special category data will be mandated to complete refresher training on data protection and information security, no less than every 2 years. The Information Governance team will monitor training compliance and follow-up with Managers/Heads of Department where areas of non-compliance are identified.

A separate refresher training package has also been produced for those staff who have been designated as non-computer users. This must be completed every two years.

6.7 *Retention of Information*

Data controllers are responsible for ensuring that data that they process is only kept for the period required to fulfil the purpose of why it was processed. This is enshrined in GDPR principle 5I.

Individual areas of the University are responsible for ensuring that they comply with principle 5I of the GDPR regarding the retention of information. Guidance will be developed by the University Information Governance team to assist relevant members of staff to determine retention periods for information they process.

Existing guidance is available on the University's website. More detailed guidance on records retention can be sought from the GDPR intranet pages.

6.8 *Subject Access*

Under the GDPR any individual can make a 'subject access request'. Subject access requests allow data subjects to access or view their personal data and to verify the lawfulness of processing.

The University has one month to respond to these requests and a copy of the information requested must be provided free of charge in the majority of cases.

For further information on the right of subject access and how it is managed at Lancaster University please refer to the subject access request webpages or contact the University's Information Governance Manager.

6.9 *Data Subject Rights*

Under the GDPR and the Data Protection Act 2018, data subjects have certain rights in relation to how their own personal information is processed. Some of these rights existed previously, such as the right to rectification; some existed but have been amended, such as the right to subject access, and some new rights have been bestowed upon individual's, such as the right of data portability.

The rights bestowed upon data subjects are:

- right to be informed;
- right of access;
- right to erasure;
- right to restrict processing;
- right to data portability;
- right to object;
- rights related to automated decision making including profiling.

Not all of these rights are absolute and some only apply in specific circumstances. More information on the rights of data subjects under GDPR and how Lancaster University fulfils these rights is available here.

6.10 *Personal Data Security Breaches*

The University is responsible for ensuring that any data that it holds is subject to appropriate technical and organisational security (Article 5(f)). This means protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage to the data. The University takes all possible steps to ensure the security of the data in its possession however; it is still possible for a breach to occur.

Personal data security breaches can happen for a number of reasons, including:

- the disclosure of confidential data to unauthorised individuals;
- loss or theft of paper records;
- inappropriate access controls allowing unauthorised access and use of information;
- attempts to gain unauthorised access to computer systems, i.e. hacking;
- confidential information being left unlocked in accessible areas;
- leaving IT equipment unattended when logged-in to a user account without locking the screen;
- publication of confidential data on the internet in error and accidental disclosure of passwords.

(This list is not exhaustive)

The GDPR places a requirement on the University to notify the Information Commissioner's Office (ICO) of a security breach within 72 hours of the University being made aware of the breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

More information is available on how the University will manage, investigate and report these types of breaches can be found in the Personal Data Security Breach Procedure.

6.11 *Data Protection Officer*

As a public authority under GDPR, the University is obligated to appoint a Data Protection Officer (Article 37(1)). The University's Information Governance Manager is the University's named Data Protection Officer (DPO).

Article 39 of the GDPR lists the responsibilities of the DPO:

- to inform and advise the University and University staff about their obligations to comply with the GDPR and other national data protection legislation;
- to monitor compliance with the GDPR and national data protection legislation, and with data protection policies, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- to advise on, and monitor, data protection impact assessments;
- to cooperate with the Information Commissioner's Office (ICO); and
- to be the first point of contact for the ICO and for those individuals whose data is processed (e.g. students, staff, etc.).

The DPO's responsibilities extend to all of the University's personal data processing activities, not just those that mandate their appointment under Article 37(1).

The contact details of the University's DPO will be published on the 'Privacy Notices' section of the University website. Lancaster University's DPO contact details have been registered with the ICO, in accordance with Article 37(7) of the GDPR.

The DPO will report directly to the Director of Strategic Planning and Governance on any data protection issues which require escalation. This will then be reported through the DCE and ultimately to the Vice-Chancellor, where appropriate.

A monthly Information Governance Assurance Report will also be presented to the Data Security and Information Management sub-Committee.

6.12 *Privacy by Design*

The University will continue to pursue a policy of 'Privacy by Design', meaning that data protection and privacy controls are integrated into processing activities and business practices. This approach will be present from the design stage through the lifecycle of the process/policy/system.

The University will ensure that the concept of Privacy by Design is made aware to all staff. This will be done by including a Privacy by Design section on the University's GDPR intranet pages and including the requirement to consider Privacy by Design in all staff training sessions.

The University will ensure that data protection impact assessments are completed where information processing is likely to result in a high risk to individuals or for any other major project which requires the processing of personal data.

For more information on Privacy by Design or the data protection impact assessment process, please see guidance on the GDPR intranet pages or contact the Information Governance team – information-governance@lancaster.ac.uk

6.13 *Data Protection Impact Assessments*

Data Protection Impact Assessments (DPIA) are a tool which can help organisations identify the effective way to comply with their data protection obligations, highlight any information risks and meet individuals' expectations of privacy. This section should be read in conjunction with the University's overall Risk Management Policy.

A DPIA must be completed where processing is "likely to result in a high risk to the rights and freedoms of natural persons"; GDPR states that a DPIA must be completed if the University are planning to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale;
- systematically monitor publicly accessible places on a large scale.

GDPR guidance on the completion of DPIAs (from the Information Commissioner's Office) states that a DPIA must be completed where the University are planning to:

- use new technologies;
- use profiling or special category data to decide on access to services;
- profile data subjects on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice (this is called 'invisible processing' and would include information gained from sites such as Facebook);
- track individuals' location;

- track individuals' behaviour;
- profile children;
- target marketing at children;
- offer online services to children;
- process data which might endanger the individual's physical health or safety in the event of a security breach.

The DPIA process will be co-owned by the Information Governance manager and the Head of IT Security.

6.14 *Data Minimisation*

The University's collection and processing of personal data will be limited to only what is necessary to achieve the purpose and aims of the processing. This policy of data minimisation will be key to the University's overall 'Privacy by Design' approach to data collection and processing.

6.15 *Use of email to share personal data*

The use of email is a ubiquitous method of communication for almost all modern businesses and organisations. However, it is accepted that email is inherently unsafe for the transfer of large volumes of personal or special category data. The University's preferred method for sharing personal data is via OneDrive/Teams/ SharePoint. Where it is unavoidable to share personal data via email, the University expects all staff to follow the principles below.

- Limit the amount of personal data shared via email – only include what is absolutely necessary. e.g. "regarding the student we discussed in the meeting earlier today", rather than "this is about Mark the Economics student from Bowland College". Consider whether initials or student number be used rather than a full name or other identifier.

- **NEVER** put personal data in the 'Subject' line of an email. If personal data is included in the email then this should be marked as **Confidential** in the 'Subject' line.

- High profile incidents have occurred where emails are sent to a large number of recipients and all are included into the 'To' or 'CC' field. Multiple recipients should be added into the 'BCC' field rather than the 'To' or 'CC' fields to limit the chances of personal data be disclosed inappropriately.

- If required to send personal or special category data either: (a) concerning several/many individuals; or (b) a significant amount of information about one individual/a small group of individuals, staff **MUST** not include this information in the body of the email. In this situation, the member of staff **MUST** put the personal or special category data in an attachment and **MUST** password protect the attachment. The password should then be communicated to the recipient via another method, e.g. telephone call.

Further information and guidance on the safe and secure sharing of personal and special category data can be found on the University intranet pages, here and here.

6.16 *Storing and sharing personal /special category data in the Cloud*

Lancaster University has specific contracts with Microsoft (for Office 365) governing data security. University data should not be stored in any other cloud storage systems unless separately approved.

Office 365 (including OneDrive, Teams, SharePoint, etc.) is hosted within the EU by Microsoft and therefore there are no limits on the storage of personal or special category information. However, staff should give due consideration to applying appropriate access controls to any personal or special category information stored within Office 365.

The University's preferred method of transfer for personal data is via the tools that Office 365 provides (e.g. OneDrive, Teams or SharePoint).

Further information about the use of cloud storage is available here.

Various services are available to staff and postgraduate researchers for research data storage. Further information is available here and here.

6.17 *Information Classification*

Lancaster University has four information classifications to help staff identify the level of security the information requires. The four classifications are: Ordinary, Confidential, Restricted and Personal.

Each of the four classifications has its own constraints on publication and requirements for access controls. For further information on the information classifications in use at Lancaster University, please see here.

6.18 *Key Performance Indicators*

The following key performance indicators will regularly be reported to the Information Security & Data Management (IS&DM) Sub-Committee, on a monthly basis to ensure measurable variables are monitored. These will include the indicators relating to data protection and freedom of information in the table below.

Annual reports will also be reported to the University Executive Board and Audit Committee.

Indicator	Measure
Staff eligible for completing Information Security training as part of corporate induction.	Eligible staff completing the training.
Staff eligible for completing Information Security refresher training.	Eligible staff completing the training.
Freedom of Information requests received.	Number of FOI requests answered within 20 working day timescale out of the total answered.
Subject Access Requests received.	Number of SARs answered within 1 month timescale out of the total received.
Number of incidents reported to Information Governance Manager.	Number of incidents reported to the Information Commissioner's Office out of the total number reported to the Information Governance Manager.
Number of other data subject rights requests.	Number of requests with which the University have complied. Where requests have not been complied with, an explanation will be given in all cases.