1. Introduction

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.

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

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.

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

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.

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

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

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. ThF2 12 T64(it)-3(cip)-4(les of)3(d)5(at)-3(

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

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 & 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 s

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

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

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

- 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.
  , rather
  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

6.16

Subject Access Req 0 0mests receiv	Number of SARs answered within 1 month timescale out of the total received

Number of incidents reported to