Data Protection Policy

Table of Contents

A. Introduction

Leeds Trinity University is committed to a policy of protecting the rights of individuals with respect to the processing of their personal data. The University holds personal information about individuals such as employees, students, graduates and others, defined as data subjects in order to undertake its business.

The University operates as a Data Controller and is required to process personal data in accordance with all current data protection legislation. The University is registered with the Information Commissioner's Office as a Data Controller under the reference Z4817023.

B. Purpose

The purpose of this policy is to outline the responsibilities of the University, its staff and its students to comply with the requirements of data protection legislation.

C. Scope

The policy applies to all staff and students of the University and in respect of all personal data that is collected, stored and processed through any activities within the University. This includes data held on both electronic and paper formats.

D. Data Protection Principles

Under data protection legislation the University is responsible for and required to be able to demonstrate compliance with the six data protection principles. Personal data must be collected and processed fairly, kept secure and not disclosed to any other parties unlawfully. Specifically, the six principles of the GDPR are:

a) Personal data must be processed lawfully, fairly and in a transparent manner in relation to individuals.

b) Personal data must be collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes.

c) Personal data must be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed.

d) Personal data must be accurate and kept up to date ensuring reasonable steps are taken to address inaccurate personal data without delay.

e) Personal data processed for any purpose must not be kept for longer than is necessary for that purpose.

f) Personal data must be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

E. Key Definitions

Personal Data - is information about a living individual, who is identifiable from that information or who could be identified from that information when combined with other data.

Special Categories of Personal Data – includes particularly sensitive personal information in respect of race, ethnic origin, political beliefs, religion, trade union membership, genetics, biometrics, health, sexual orientation.

Data Processing – includes collecting, recording, storing, organising, editing, combining and erasing of personal data.

Data Controller – Where Leeds Trinity University determines the purposes and means of processing of personal data it is considered to be the data controller of that data and has legal obligations as a result.

Data Subject – is an individual whose personal data is being processed.

F. How the University complies with GDPR

Ensuring an appropriate lawful basis for processing

In order for the University to process personal data it must meet one of the following conditions which provide the legal basis for processing:

a) The data subject has given their consent
b) The processing is required to fulfil a contract between the University and the data subject (e.g. a student studying at the University or a staff member being employed by the University)
c) It is necessary due to a legal obligation
d) It is necessary to protect someone's vital interests
e) It is necessary for performing a task (usually by an official authority) carried out in the public interest
f) It is necessary for the legitimate interests of the data controller or a third party and does not interfere with the rights and freedoms of the data subject.

Where the processing involves special category personal data the lawful basis for the processing must also be disclosed to the data subject at the time their data is collected.

Privacy notices

In order to demonstrate fair and transparent processing of personal data, the University is required to provide data subjects with privacy information.

The University makes privacy notices available to enquirers, applicants, students, alumni and staff as they are asked to provide their personal data. The privacy notices are also available on the University website for data subjects to view at any time.

In the event of the University wanting to process personal data beyond the scope of existing privacy notices, then separate and additional privacy information will need to be provided to data subjects before this can take place. Staff should seek guidance about the required content of a privacy notice from the Data Protection Officer where additional privacy information is required.

Data retention

The University is required to ensure that it only retains personal data for as long as is necessary to fulfil the original processing for which it was collected. The University manages the retention of personal data through setting retention periods after which data will be deleted or archived. Retention periods are set based on legal and regulatory requirements and good practice guidance.

Staff must comply with the retention periods by ensuring that electronic records are deleted once data is no longer necessary. Paper based records should be disposed of in confidential waste.

If data is fully anonymised it is acceptable to keep beyond retention periods for statistical purposes. Further details of the retention schedule used by the University can be found here.

Subject access requests and upholding data subject rights

Data protection legislation gives data subjects rights to access personal information that is held by the University about them. The University must respond to all subject access requests and do so in line with the timescale for response which is within one month of when the request is received. Where a request is particularly complex and it is not realistic for the University to respond within one month the response time can be extended but the data subject must be informed of this. Data subjects and University staff can see further information on the University's policy for handling subject access requests here.

Data subjects also have a number of other rights under the GDPR which the University must comply with, these include:

a) **Right to rectification** – the University must allow data subjects to correct inaccuracies in the personal data that is held about them. The aim is to allow staff and students to review a range of their personal data that is held by the University using systems that permit them to access and update their personal data. Data subjects are also informed by means of privacy notices and other communications how to notify the University should any personal information held be incorrect or incomplete.

b) **Right to erasure** - Individuals have the right to have their personal data erased. This includes where consent is the lawful basis for holding the data and the individual withdraws their consent as well as where processing the personal data is no longer necessary for the purpose for which it was originally collected and processed.

c) **Right to restrict or object to processing** - Individuals have the right to restrict the processing of their personal data or object to the processing of that data in certain circumstances. This could apply where the University no longer has a contractual or legitimate need to process the personal data.

d) **Right to data portability** – This right allows individuals to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way. The University will provide an individual (upon request) with the personal data that they have given to the University.

e) **Rights related to automated decision making** – The University does not undertake any decision making solely by automated means without any human involvement. Data protection legislation requires that data subjects are notified of whether any automated processing takes place and provides strict guidance on when this is permitted.

Third party personal data requests

Where requests for personal data are received from third parties (any party other than the data subject) the University will only release personal data for legitimate reasons subject to the following conditions all being met:

a) The processing is for a legitimate sharing activity as outlined by the applicable privacy notice; or is to protect the vital interests of the data subject such as in an emergency situation where the subject may be harmed by not releasing the personal information; or the University has a legal obligation to share the personal information such as in the detection or prevention of crime.
b) The identity of the requesting third party has been identified and confirmed as legitimate
c) The data is shared with the subject in an appropriately secure manner.

In no other circumstances should any personal information be released by the University without the consent of the data subject. Further information is also provided in the University's subject access request policy, details are available here.

Data security

It is essential to ensure that personal data that is held is kept securely by all members of the University to prevent any unauthorised disclosure. Data security should be upheld in conjunction with the requirements of the following policies: acceptable use policy, access control policy, mobile device and remote working policy, password usage and management policy, information classification policy. Staff can consult these policies here.

International transfers of data

Data protection legislation imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

Leeds Trinity University will only transfer personal data outside of the EU where the organisation receiving the personal data has provided adequate safeguards in compliance with data protection legislation. The University ensures that all corporate systems that may be hosted on servers outside of the EU meet all appropriate safeguards.

Data protection by design

Data protection legislation requires that organisations ensure data protection is carefully considered and evaluated when introducing any significant new processing activities involving personal data. This can include implementing new IT systems for storing or accessing personal data, embarking on a new data sharing initiative, processing personal data for new purposes.

The University requires that staff undertake a Data Protection Impact Assessment (DPIA) ahead of making any such significant changes. This will serve to identify any potential concerns at an early stage so that the design will protect the privacy and rights of data subjects. More details of undertaking a DPIA can be found on the staff Data Protection and IT Security intranet page.

The University's Data Protection Officer should be consulted who will confirm if the DPIA and any risks reviewed can allow the significant processing change to take place.

Personal data breaches

The University is required under data protection legislation to investigate any confirmed or suspected data protection breach promptly. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

The University will review the impact of the breach incident and undertake the following;

- notify the Information Commissioners Office (ICO) of the breach incident within 72 hours for all reportable incidents,
- review what process or policy improvements should be made to mitigate the risk of reoccurrence,
- update the data protection breach register to record the incident and action taken.

Further details of the University policy on data protection breaches can be found in the associated policy here.

Staff responsibility

The University requires all staff to ensure that they have a suitable understanding of data protection in order to undertake data processing as part of their work securely and in compliance with data protection legislation.

Staff are encouraged to seek further support by discussion with their line manager and from reviewing support materials provided by the University on the staff intranet. The ICO website (www.ICO.org.uk) also provides guidance on compliance with data protection legislation. For more complex matters requiring specific support staff should consult the University Data Protection Officer.

Staff are expected to comply at all times with the requirements of the Data Protection Policy. Failure to do so could lead to formal University procedures, including disciplinary action where appropriate.

G. Evaluation and review

This policy will be formally reviewed every year by the Data Protection Officer. In addition, the effectiveness of this Policy will be monitored as necessary on an on-going basis to ensure it is compliant with relevant legislation.

This policy was last updated in May 2023.

Published date: June 2023
Review date: May 2024