University of York

Data Protection Policy

1. Introduction

This Data Protection Policy sets out how the University of York handles the Personal Data of its students, staff, alumni, research participants, suppliers, website users and other third parties.

2. Scope

This Policy applies to all Information Users i.e., University staff, students, associates, and anyone else who may access, use or manage University information (e.g., visitors, contractors, partners). It extends to all situations where the University of York is the data controller or a data processor of Personal Data and applies to all Personal Data processed regardless of the media on which the data is stored.

3. Roles and responsibilities

The **Senior Information Owner (SIO)** has overall responsibility for data protection compliance.

Information Owners are responsible for ensuring that Personal Data in their area is processed in accordance with this Policy and any associated regulations, policies, and procedures. Information Owners are responsible for ensuring their staff complete mandatory data protection training and for appointing Information Champions.

Information Champions are responsible for monitoring mandatory training completion. They are also responsible for maintaining information asset registers and for providing a local point of contact for queries, liaising with the Data Protection Officer and Legal Services as required.

Information Users are responsible for the information they use and must follow relevant regulations, policies, and procedures. They must also complete mandatory data protection and information security training.

The **Data Protection Officer** (DPO) is responsible for overseeing the University's compliance with data protection legislation. The DPO has those responsibilities laid out in Article 39 of the UK General Data Protection Regulation (UK GDPR). The DPO has a reporting line to the SIO. Matters may also be referred to Audit and Risk Committee where appropriate.

4. Data Protection Principles

The University will ensure Personal Data is:

a. processed lawfully, fairly and in a transparent manner;
b. collected only for specified, explicit and legitimate purposes;
c. adequate, relevant, and limited to what is necessary in relation to the purpose for which it is processed;
d. accurate and where necessary kept up to date;
e. not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed;
f. processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

The University will maintain appropriate records to demonstrate compliance with these principles.

5. Data Protection by design and default

The University is committed to the principle of data protection by design and default. Privacy and data protection issues are fully considered during system, service, product, or process design and throughout the lifecycle of the data processing arrangement.

In support of this requirement, all Information Users are responsible for screening proposed data processing activities against the Data Protection Impact Assessment Screening Questions and for working with Information Champions to conduct Data Protection Impact Assessments where required.

In addition, all staff must use the minimum amount of data necessary for the purpose and consider the use of anonymised data or pseudonymised data as appropriate.

6. Breach management

The University maintains a breach management procedure and reports qualifying breaches to the Information Commissioner's Office within 72 hours of identification as required by the UK GDPR. All Information Users are responsible for familiarising themselves with the breach management procedure and for reporting suspected or actual breaches to the DPO immediately on identification. Information Users must also preserve all evidence relating to the potential Personal Data breach whilst an investigation is ongoing.

7. Data sharing

The University will ensure data sharing is undertaken in accordance with the UK GDPR. All Information Users are responsible for identifying situations where data is to be shared outside the University of York or its wholly owned or controlled subsidiaries. Proposed sharing arrangements must be brought to the attention of the University's Data Protection Officer at dataprotection@york.ac.uk so that appropriate safeguards can be put in place. Where data is to be transferred to third party service providers, the University will ensure that appropriate contracts are put in place to meet Article 28 requirements. All Information Users are responsible for ensuring that services are procured in accordance with the University's tender process.

8. International transfers

The University will ensure all data transfers outside of the United Kingdom are conducted in accordance with the UK GDPR. All Information Users are responsible for identifying situations where data is to be transferred internationally. Proposed transfers must be brought to the attention of the University's Data Protection Officer at dataprotection@york.ac.uk so that appropriate safeguards can be put in place.

9. Subject rights

The University maintains procedures to enable individuals to exercise their rights under data protection legislation i.e.,

- Right to be informed;
- Right of access;
- Right to rectification;
- Right to erasure;
- Right to restrict processing;
- Right to data portability;
- Right to object;
- Rights in relation to automated decision making and profiling.

All Information Users are responsible for familiarising themselves with the University's subject rights procedures and for forwarding rights requests to dataprotection@york.ac.uk immediately on receipt.

10. Data security

The University has put in place appropriate technical and organisational measures to protect Personal Data. These measures will be kept under review. All Information Users are required to comply with the University's Information and Records Management Policy, Information Security Policy and associated guidance.

11. Recordkeeping

The University will maintain full and accurate records of its data processing activities. This will include records of consent and procedures for obtaining consent. Records will be retained in line with the University's approved retention schedules. All Information Users are responsible for adhering to these retention schedules and for complying with the University's Information and Records Management Policy.

12. Training

Staff are required to complete mandatory online data protection training. In addition, the University will offer bespoke training to groups of Information Users as appropriate.

13. Audit

The University will conduct periodic audits to assess compliance with this Policy and the Data Protection Act 2018 and UK GDPR.

14. Changes to this Policy

This Policy is kept under regular review. This version was last updated on 9 September 2021.

Historic versions can be requested via dataprotection@york.ac.uk.