



Records of Processing Activities (ROPA)

Information Governance & Data Protection

Summary		
This Record of Processing document is to meet the requirements of Information Governance best practice and the Data Protection Act 2018. It describes the type of data we use, why and where data maybe shared.		
Scope		
This document applies to all staff, associates, students, research participants and visitors across all sites that the University of Exeter operates from.		
Document Control		
Document type	Information Governance Record of Processing Activity	
Document owner	Information Governance Manager & Data Protection Officer	
Division	Compliance, Governance and Risk	
Lead contact	Information Governance Manager & Data Protection Officer	
Document status	live	
Version	v2.1	
Approved by	Senior Information Risk Officer Information Strategy Group	Date
Date of publication		Next review date

Contents

Details of the Organisation	3
Purposes of Processing	3
Recipients and transfers	4
Retention	5
Technical and Organisational Security	5
Lawful Purpose for Processing	5

Details of the Organisation

The University is a registered data controller with the ICO registration number Z5785872.

The University's Senior Information Risk Owner, details can be found [on our senior staff pages](#).

The University's data protection officer details can be found [here](#).

Email: informationgovernance@exeter.ac.uk

Purposes of Processing

The University processes data to enable the fulfilment of its obligations as an Educator, Research, Service providers, Business Partners to facilitate these processes to:

- Services to enable and support the delivery of education to students
- Management and fulfilment of research activity
- Clinical Trials
- Research
- Staff Recruitment and administration
- Perspective Student engagement
- Statutory and legal obligations
- Financial administration
- Security of property, staff, students, visitors and infrastructure
- Facilitating the health, safety and wellbeing of staff, students and associates.
- Marketing and promotion of the University and events
- Alumni engagement
- Training
- Protection through testing and support service due to covid-19 pandemic

The University works with and for individuals who fall into one or more of the following categories:

- Alumni
- Associates
- Business and Industry Partners
- Complainants and Enquirers
- CCTV capture of persons on site
- Employees and contracted personnel
- Enquirers
- External third parties
- Exchange Students
- Former Employees including retirees
- Failed applications Students/Staff
- Enquirers/complainants
- Parents, guardians, and carers
- Prospective Employees
- Prospective Students
- Research Participants
- Students
- Suppliers of goods and services
- Withdrawn Students
- Visitors
- Volunteers
- Website users
- Users of University Services and events

All these activities require the collection and use of the personal data of individuals that may include:

- Basic personal identifiers
- Next of kin emergency contact
- Student record data (attendance & academic work, attainment)
- Financial data
- Imagery (photo, video, CCTV)
- Contracts
- Disciplinary/Grievances Investigations
- Employment record
- Vetting checks
- Qualifications and professional memberships
- Criminal information
- Lifestyle and social information
- Trade Unions
- Health data
- Ethnicity/nationality
- Equality information
- Research functions
- IP and security data

The University collects data whilst providing IT functionality, this is incidental as part of providing a network for usage. This enables the university to protect the network and the processing of data and usage across the estate of the University of Exeter.

Due to the nature of research a significant amount of personal and sensitive data maybe collected for research participants. Such data is collected for the defined purpose of the research and conducted in line with the University's ethics policies.

More details about research ethics at the University of Exeter can be found [on our ethics web pages](#).

The University always aims to minimise the use of personal data and only collects details which are necessary to carry out its legal duties or specific functions which you will be notified of at the point of data collection. You can see an [index of our privacy notices on our website](#).

Recipients and transfers

The University works with several key partners across the globe to provided services and support to staff and students. The University will notify individuals of specifics at the appropriate time. There are several common categories of data recipient which include:

- Suppliers and service providers
- Partner Universities
- Accommodation partners
- Regulatory and Government departments
- Local councils
- Law enforcement
- Awarding bodies
- Debt Collection
- Student support partners (abroad and UK)
- Partner Employers
- Research councils
- Agents assisting with applications
- Overseas governments to assist with visa applications and similar
- Previous or new Employers
- Third party agencies such as HESA
- Student Guild
- International Language support (INTO)
- Research Participants
- Third party collaborators/partnerships
- Pensions

Due to the way such services are arranged it is not possible to provide a comprehensive list of third countries. Many of these transfers will be conducted for specific purposes, many of which are instigated by the data subject. The University provides lists of such services within the relevant

privacy policies published [on our website](#) which go into details specific to the relevant service users. Where data is processed in a third country, the University will ensure specific legal agreements are in place (Standard Contractual Clauses). We will also always look to minimise the required data to share.

Retention

The University maintains a comprehensive retention schedule which is available [on our website](#). legislation and the University's [Information Retention Policy](#).

Technical and Organisational Security

The University takes the security and integrity of its data and systems incredibly seriously. Due to the nature of the threats posed in this area the University will not disclose details of the specific measures taken to protect our networks against criminal activity. This is to prevent such details being used to triangulate attack vectors against university systems.

In addition to network security there are several other tools and techniques which are employed by university employees during the gathering of data. The data uses at the University are diverse and policies, procedures, technologies, and guidance are available to staff and students depending on their needs.

The Secure Data Research Hub, has been built to meet the requirements of the DSPT, and towards ISO27001 requirements.

Lawful Purpose for Processing

The University processes data in the following categories:

	Lawful Purpose	Special Category
Recruitment	Consent Legal obligation	Art (9) Employment
Employee /Associate	Contract Legal obligation Consent Legitimate Interest	Explicit Consent Art (9) Employment
Perspective Student	Consent Legal obligation	
Student	Contract Legal obligation Public Task Legitimate interest	Explicit Consent
Visitor	Public Task Consent	
Research Participant/Trials	Consent Public Interest	Explicit Consent
Alumni (Marketing)	Consent	Explicit Consent
Alumini	Legitimate Interest	
Student Guild	Legal obligation	
Contractors	Consent Legal obligation	

Brenda Waterman
Information Governance & Data Protection Officer
June 2022