Information Sharing Policy

Version:	**1**
Dated:	**16 May 2018**
Document Owner:	**Information Governance Manager**

Revision History

Version	Date	Revision Author	Summary of Changes
V 0.1	May 2018	R. Platt	Initial draft
V 1	May 2018	R. Platt	Approved Version

Approval

Version	Approval Board	Date of Approval
V 1	Information Governance & Security Steering Group	May 2018

Table of Contents

1. Introduction: 4
2. Scope 4
3. Definitions 4
3.1 Data Controller 4
3.2 Data Processor 4
3.3 Joint Controllers 4
4. Responsibilities 5
4.1 Information Users 5
4.2 Researchers and Principal Investigators 5
4.3 Senior Information Officers (SIO) 5
4.4 Managers and Supervisory Roles 5
4.5 Information Asset Owners (IAO) 5
4.6 System Owners 5
4.7 Legal Services 5
5. Policy 5
6. International Transfers 6
7. Relationship to existing policies 7

1. Introduction:

1.1 The work of the University requires the sharing of information between staff, between staff and students, and between staff and (external) third parties. This policy aims to minimise the risk of loss, unauthorised disclosure, modification or removal of information maintained by the University whilst seeking to maintain the open nature of the organisation.

2. Scope

This policy covers the sharing of information and the controls used to share such data. It covers all forms of information, whether held and shared in hardcopy or electronic format.

This policy covers the sharing of information with processors or joint data controllers, information is shared and processed with many third parties including, but not limited to, collaborative research partners, system suppliers, service suppliers, other Universities and partner organisations.

3. Definitions

The definitions are as defined in the General Data Protection Regulation (GDPR)

3.1 Data Controller

A controller determines the purposes and means of processing personal data and needs to ensure that, where a processor is used, a legally binding contract is in place.

'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

3.2 Data Processor

A processor is responsible for processing personal data on behalf of a controller and they are required to maintain records of personal data and processing activities. They will have legal liability if they are responsible for a breach.

'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

3.3 Joint Controllers

Joint Controllers are required where both parties need to make decisions about the processing; this needs to be clearly understood and agreed in an appropriate contract/agreement.

Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

4. Responsibilities

The University of Exeter is the 'data controller' and the Council of the University is ultimately responsible for compliance with current data protection legislation.

4.1 Information Users

All members of the University are responsible for complying with all relevant data protection legislation and this policy. Where a decision is taken to share information with relevant individuals or third parties, it is the responsibility of those releasing the information to ensure that the recipient understands the confidentiality of the information and will abide by the provisions of any data sharing agreement.

4.2 Researchers and Principal Investigators

Researchers must ensure all sharing and collaborative work has appropriate controls in place and follows the advice in the Research Toolkit. They should ensure compliance with the Open Access Research and Research Data Management Policy and any requirements of the funding body. PI's are responsible for ensuring that all members of their research teams understand the processes and agreements that are in place for information sharing during the project.

4.3 Senior Information Officers (SIO)

Directors of College Operations and Directors of Professional Services have the responsibility of overseeing compliance and developing good data protection practice within their designated areas.

4.4 Managers and Supervisory Roles

Managers and all employees in supervisory roles should ensure that information is only shared with relevant individuals and where a data sharing agreement is in place, that the conditions are met.

4.5 Information Asset Owners (IAO)

Information Asset Owners are responsible for their information assets and for authorising data sharing with relevant individuals or third parties. They need to ensure that appropriate controls are in place, such as data sharing agreements or contracts.

4.6 System Owners

System owners/administrators are responsible for ensuring systems that hold information have appropriate access controls in place to ensure information is only shared with individuals or third parties approved by the IAO and in line with any data sharing agreements.

4.7 Legal Services

The Legal Services is responsible for providing legal advice on contracts and data sharing agreements and will work closely with the Information Governance Office where required on contracts that involve the sharing of personal data.

5. Policy

5.1 The University of Exeter is a Data Controller: it makes decisions about how and why data is processed and is accountable for ensuring compliance with relevant legislation. As a Data Controller, the University processes much of its own data and does not usually require a data processor or data sharing agreements where processing remains in house.

5.2 The University may also act as a Data Processor, where this is in place the Data Controller is responsible for defining each party's responsibilities and liabilities. Staff must ensure before signing these agreements that the University can meet all of the requirements and that the University is only accepting the appropriate level of liability.

5.3 All staff must ensure that whenever the University uses a processor to handle personal data on their behalf, there must be in place a written contract that sets out each party's responsibilities and liabilities.

5.3.1 Contracts must include certain specific terms as a minimum, such as requiring the processor to take appropriate measures to ensure the security of processing and obliging it to assist the controller in allowing individuals to exercise their rights under the GDPR.

5.3.2 The contract must meet GDPR requirements whenever any personal data will be shared. There is an expectation that EU or ICO standard clauses will be provided and staff should ensure that contracts meet all current requirements.

5.3.3 Controllers are liable for their compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected.

5.3.4 Processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply.

5.3.5 Using clear and comprehensive contracts with processors helps to ensure that everyone understands their data protection obligations and is a good way to demonstrate this formally.

5.4 All staff must ensure that whenever the information sharing is outside the EEA that appropriate controls will be in please as defined in section 6 of this policy and in compliance with the GDPR requirements in Chapter V.

6. International Transfers

6.1 The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.

6.2 These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

6.3 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.

6.4 Transfers may be made where the Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection.

6.5 You may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

6.6 Adequate safeguards may be provided for by:

- a legally binding agreement between public authorities or bodies;

- standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority (the ICO) and approved by the Commission;
- compliance with an approved code of conduct approved by a supervisory authority (the ICO);
- certification under an approved certification mechanism as provided for in the GDPR;
- contractual clauses agreed authorised by the competent supervisory authority (the ICO); or
- provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority (the ICO).

7. Relationship to existing policies

7.1 This policy should be used in conjunction with other relevant University policies and documents including but not limited to:

- Privacy and Personal Data Protection Policy
- Information Security Controls policy
- University Data Classification Policy
- Open Access Research and Research Data Management Policy