DATA PROTECTION POLICY

Operational Owner:	James Newby –Data Protection Officer
Executive Owner:	Sarah Litchfield – Senior Information Risk Officer
Effective date:	25th May 2018
Review date:	May 2021
Related documents:	Information Security Policy

Approval History

Version	Reviewed by	Approved by	Date
1	Updated version of policy reviewed by James Newby	EB	24 May 2018

1 Introduction

1.1 Purpose

1.1.1 Data protection legislation, including the General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 applies to all information relating to an identified or identifiable living individual. This is defined as personal data within data protection legislation.

1.1.2 The University of Surrey takes the protection of all personal information extremely seriously and is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal information.

1.2 Scope

1.2.1 The University of Surrey holds and processes information about its current, past or prospective employees, prospective students, applicants, current students, alumni and others who are defined as data subjects within data protection legislation

1.2.2 The University processes personal information for a variety of reasons which it defines within its Privacy Notices.

These purposes include:

- Administration of the student application process
- Academic administration
- Managing Human Resources processes, such as applications, performance management, training and development
- Administration of financial aspects of an individual's relationship with the University
- Management of use of facilities and participation in events
- Enabling effective communications with staff and students
- Operation of security, disciplinary, complaint and quality assurance processes and arrangements
- Support of Health, Safety and Welfare requirements
- Production of statistics and research for internal and statutory reporting purposes.
- Fundraising and Marketing

1.3 Definitions

1.3.1 Data Protection Officer – The University's responsible officer for data protection compliance.

1.3.2 Data Subject - a natural person whose personal data is processed by the University of Surrey or

by an appointed data processor.

1.3.3 Data Controller - the entity that determines the purposes, conditions and means of the processing of personal data.

1.3.4 SIRO – Senior Information Risk Owner, the University's Legal Counsel.

2 Policy

2.1 Principles

2.1.1 Anyone who processes personal information within the University must comply with the principles of data protection. The Principles define how data can be legally processed. Processing means any operation which is performed on personal data or sets of personal data, by automated or manual means such as collecting, recording, organising, storing, adapting, altering, consulting, using, disclosing, combining, restricting, erasing or destroying.

2.1.2 The principles of data protection state that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (although certain other safeguards must be in place as defined within the GDPR);

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods when processed only for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of appropriate measures to protect the rights and freedoms of data subjects;

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

2.1.3 The University shall be responsible for, and be able to demonstrate compliance with data protection legislation.

2.2 Roles and Responsibilities

The University, as data controller, is responsible overall for demonstrating compliance with data protection legislation and meeting the accountability and transparency obligations within the legislation.

The University has an Information Compliance Unit who are responsible for co-ordinating day to day data protection functions.

Senior Managers have a responsibility to ensure compliance with data protection legislation and this policy, and to develop and encourage good information handling practices within their areas of responsibility

All staff have a responsibility to ensure they process personal data in accordance with the data protection principles and other requirements of data protection legislation

Academic and academic-related staff are responsible for the conduct in data protection matters of the students they supervise.

The University of Surrey notifies annually to the Information Commissioner's Office regarding the processing of personal data that it undertakes. This notification uses data from the Data Asset Registers maintained by Information Asset Owners throughout the University

The Information Compliance Unit will perform periodic audits to ensure compliance with this policy and to ensure that the notification to the Information Commissioner is kept up to date and appropriate accountability can be demonstrated

2.3 Procedures

2.3.1 Information Asset Owners

Each area of the University that processes personal data will assign a member of staff to be a named Information Asset Owner.

In Information Asset Owner will be a member of staff who manages an information or data asset and has the power to make decisions about how that information is managed

Information Asset Owners will work with the Information Compliance Unit to disseminate guidance and information relating to data protection and good information handling practices, as well as managing breach reporting within their area and maintaining the appropriate registers to demonstrate accountability in relation to data protection.

2.3.2 Record of processing

Information Asset Owners will be responsible for recording data assets within the University's data asset register(s) and for maintaining this register.

2.3.3 Privacy Impact Assessments

All major data processing activities, especially new processing of personal data or adaptations of

existing methods of processing, are risk assessed using the University's Privacy Impact Assessment process to ensure that the proposed processing complies with the requirements of data protection.

Templates and guidance provided by the Information Compliance Unit should be used to complete the Privacy Impact Assessment.

2.3.4 Data subject rights

The University will comply with all data subject rights, as appropriate in relation to the processing it undertakes.

These rights are:

- Transparency of processing
- Right of access to personal data
- Right of rectification of inaccurate personal data
- Right of erasure
- Right to restriction of processing
- Right to data portability
- Right to object to processing where it is processed in the following way:
    - for direct marketing purposes
    - for scientific/historical/research/statistical purposes
    - based on legitimate interest grounds
    - necessary for the performance of a task carried out in the public interest
- Right to object to automated individual decision making, including profiling

Transparency of processing

Wherever personal data is collected for a new purpose, the Information Asset Owner responsible for that data will ensure a Privacy Notice is created and shared with data subjects.

This Privacy Notice will include:

- Name of data controller and contact details
- Contact details of the University Data Protection Officer

- Purposes of processing the data
- Legal basis of processing
- Transfers outside the EU
- Length of time for which data will be retained
- Data subject rights in relation to the data
- Recipients of the data
- Statutory or contractual requirements to provide the data
- Any automated decision making including profiling
- Right to complain to the Information Commissioner's Office (ICO) if data is not processed in accordance with data protection principles.

Information Asset Owners should use guidance and templates made available by the Information Compliance Unit to create Privacy Notices unless otherwise justified by the circumstance.

2.3.5 **Subject Access Requests**

Data Protection Legislation gives data subjects the right to access any personal information held about them by the University of Surrey.

Any person can exercise this right by submitting a Subject Access Request form, available from the Information Compliance Unit. Any formal subject access request must be responded to within the 30 calendar days, or appropriate additional timescale as laid down by data protection legislation, and must be notified to the Information Compliance Unit as soon as they are received.

2.3.6 **Data sharing**

All sharing of personal data with third parties will be subject to the appropriate controls as laid out in data protection legislation.

Repeated or ongoing data sharing arrangements must be covered by an appropriate data sharing or processor agreement which must be signed off as follows:

- The University's Data Protection Officer will sign off data sharing agreements with third parties within the European Economic Area (EEA) which use standard clauses supplied by the Information Compliance Unit (ICU) or the SIRO
- The SIRO will sign off all other data sharing agreements.

2.3.7 **Use of personal data within research**

Where research involves the processing of personal data, the Chief or Principal Investigator will be considered to be the relevant Information Asset Owner for the data.

All requirements of this policy relating to processing of personal data should be adhered to alongside the University's research good practice requirements.

Use of personal data for research purposes will be subject to the appropriate safeguards as specified within the data protection legislation. In particular, personal data should be limited to the minimum amount of data which is reasonably required to achieve the desired academic objectives. Wherever possible, personal information should be anonymised or pseudonymised so that the data subjects cannot be identified.

Students should only obtain or use personal information relating to third parties for approved research or other legitimate University-related purposes with the knowledge and express consent of an appropriate Information Asset Owner or member of staff who is responsible for their supervision.

3 Governance Requirements

3.1 Implementation / Communication Plan

3.1.1 This policy is communicated to all staff as part of the University induction process.

3.2 Exceptions to this Policy

3.2.1 There are no exceptions to this policy. Data Protection Legislation requires that all processing of personal data within the University be subject to an appropriate policy.

3.4 Review and Change Requests

3.4.1 This policy will be reviewed annually.

Next review due in May 2019.

3.5 Legislative context

3.5.1 This policy is underpinned by the General Data Protection Regulations and the UK Data Protection Act 2018.

3.6 Stakeholder Statements

A stakeholder analysis should be undertaken when creating or reviewing a policy. This must take account of Equality and Health & Safety but should also include consulting any other areas which might have relevant input, or be significantly impacted.

3.6.1 Equality: This policy relates to the management of data and applies to all employees of data controllers. No adverse equality impacts are identified.

3.6.2 Health & Safety: No new health and safety implications arise from this policy.

3.6.3 Other: None.