UNIVERSITY OF SUSSEX

Planning, Information Management and Compliance

DATA PROTECTION POLICY

1. OVERVIEW AND PURPOSE

1.1 This University policy relates to personal data protection and reflects the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 which apply to any processing of personal data[1] that is carried out by organisations operating within the European Union, and/or those that offer goods or services to individuals within the European Union.

1.2 The GDPR is applicable to both data 'controllers' and 'processors'[2] of personal data.

1.3 The GDPR applies in the UK as tailored by the Data Protection Act 2018.

1.4 The University has a duty to comply with the principles and requirements of the GDPR, including implementing data protection policies and ensuring data protection considerations are at the forefront of University activities involving the processing of personal data.

1.5 This purpose of this policy is to:

- Lay out the principles of the GDPR and define key terms;
- Make clear the responsibilities within the University in relation to compliance; and
- Outline the rights of data subjects.

2. SCOPE

2.1 This policy applies to all processing of personal data by the University.

2.2 This policy applies to all staff and others processing personal data controlled by the University, either remunerated or not, including:

- Senior managers, officers, and directors;
- Employees (whether permanent, fixed-term, temporary, or casual);
- Contract, seconded, and agency staff;
- Volunteers, apprentices, and interns; and

[1] The definition of personal data under the General Data Protection Regulation has been expanded (from the Data Protection Act 1998) to include a wider range of personal identifiers, including online identifiers (such as an IP address), in order to reflect changes in technology and the way information about data subjects is collected by organisations.

[2] A 'controller' determines the purposes and means of processing personal data and a 'processor' is responsible for processing personal data on behalf of a controller

- Others associated with (i.e. performing services for or on behalf of) the University (including agents, sponsors, contractors, representatives, consultants, and other service providers), or who are otherwise deemed to be covered by this policy by the Chief Operating Officer.

2.2 Except where a student is also an employee of the University, or processing personal data as a part of the University (e.g. as part of research work), this policy does not apply directly to students, but students should be aware of their rights as data subjects and the University's responsibilities as a controller of their personal data.

2.3 Third parties that process personal data on behalf of the University should also have regard for this policy.

3. RESPONSIBILITIES

3.1 The University's Information Governance Committee (IGC)

3.1.1 The Committee is responsible for supporting and driving the broader Information Governance/Security agenda at the University, as well as providing assurance that effective best practice mechanisms are in place across the University.

3.1.2 Within the context of data protection, the Committee is responsible for:

- Acting as the primary decision-making authority on Information Governance matters, and Committee members are expected to act as ambassadors across the University for Information Governance;
- Reviewing, contributing to, and approving all Information Governance-related policies, processes, and standards;
- Ensuring provision of resource to deliver, and inputting into, Information Governance strategy; and monitoring performance;
- Acting as a point of escalation for related issues;
- Reviewing regulatory obligations and having oversight of legislative requirements in relation to the General Data Protection Regulation; and
- Having oversight of data breaches and information security incidents.

3.1.3 The Committee is responsible for ensuring that the Data Protection Officer is able to undertake their role effectively and, in particular, must ensure that they have adequate resources, in terms of staff and access to training. In addition, the Committee should ensure that the Data Protection Officer has access to all data processing that occurs across the University.

3.2 The Data Protection Officer (DPO)

3.2.1 Under the GDPR, the University is required to appoint a Data Protection Officer (DPO).

3.2.2 The DPO is responsible for monitoring internal compliance with the GDPR, informing and advising on data protection obligations, providing advice in relation to Data Protection Impact Assessments, and acting as a contact point for data subjects and the Information Commissioner's Office (ICO).

3.3 **The Senior Information Risk Owner (SIRO)**

3.3.1 The Senior Information Risk Owner (SIRO) is a senior management team member who is familiar with information risks and provides the focus for the management of information risk at that level.

3.3.2 The SIRO is responsible for leading a culture of good Information Management, and for providing assurance that information risk is being managed appropriately and effectively across the organisation and for any services contracted for by the organisation.

3.4 **The University (Data Controller)**

3.4.1 The University is responsible for ensuring that the appropriate technical and organisational measures are put in place to meet the requirements of accountability (one of the data protection principles) in relation to personal data – i.e.:

- adopting and implementing data protection policies and appropriate security measures;
- ensuring data protection is incorporated into 'business as usual' processes;
- ensuring appropriate arrangements (and data sharing agreements, where necessary) are in place with organisations that process personal data on the University's behalf;
- maintaining documentation of processing activities;
- recording and reporting personal data breaches;
- carrying out Data Protection Impact Assessments for uses of personal data that may present a risk to the rights of data subjects;
- Reviewing and updating measures and policies in place as required;
- Creating a culture that values and considers privacy issues; and
- Ensuring staff are trained in data protection and aware of their responsibilities.

3.5 **Data Processors**

3.5.1 The GDPR places specific legal obligations on processors; i.e. to maintain records of personal data and processing activities.

3.5.2 Where the University engages with a third party processor, their obligations and the University's expectations regarding data protection (i.e. adherence to the University's policy and the GDPR) should be made clear. This may be in the form of a Data Sharing Agreement or by carrying out a due diligence exercise to gain assurance of the processor's data protection mechanisms.

3.5.3 Data Processors have legal liability if responsible for a data breach.

3.6 **Staff**

3.6.1 All staff are responsible for familiarising themselves with this policy and, in particular, must ensure:

- That adequate safeguards are in place to protect data they process and that data which is no longer required for use or retention is disposed of safely and securely, and

- that they are only processing data for the purpose outlined in the University's ICO register entry and the University's privacy policies.

3.6.2 Staff are responsible for ensuring that they complete all training as required by the University.

3.6.3 Staff are responsible for ensuring they report any personal data breaches they become aware of immediately via the correct process (see Related Guidance for a link to the University's breach reporting process).

3.7 **Information Asset Owners (IAOs)**

3.7.1 The IAOs work with the DPO and Information Management team to understand what information is held within their School or Professional Services Directorate (or area), what is created or added, how information is moved, who has access to it and why. IAOs are expected to ensure that the University's Information Asset Register is accurate and up to date, and should understand and address any risks to information assets in their area.

3.7.2 IAOs should act as a point of contact within their School or Directorate for basic data protection queries.

4. **POLICY DETAILS**

4.1 **Data Protection Principles**

4.1.1 Under the GDPR, the principles relating to the processing of personal data are as follows:

4.1.2 Personal data shall be:

- processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

- 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 ('storage limitation'); and

- 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 ('integrity and confidentiality').

4.1.3 The data controller is responsible for, and must be able to demonstrate compliance with, the above ('accountability').

4.2 Personal Data

4.2.1 The GDPR defines personal data as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'

4.2.2 Some particularly sensitive personal data is classed as 'special categories' data, including racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

4.2.3 In order to lawfully process special category data, you must identify both a lawful basis under Article 6 (as set out in paragraph 4.3.2 below) and a separate condition for processing special category data under Article 9. These do not have to be linked.

4.3 Data Processing

4.3.1 Data 'processing' is defined by the GDPR as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.'

4.3.2 There must be a valid lawful basis for processing personal data, and this should be determined before data is processed, documented, and included in the relevant privacy notice. Under GDPR, six lawful bases are available:

- Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

- Legal Obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

- Vital Interests: the processing is necessary to protect someone's life.

- Public Task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

- Legitimate Interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

- Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

4.4 **Data Subject Rights**

4.4.1 The GDPR provides the following rights for individual data subjects:

- The right to be informed: about the collection and use of their personal data, including the purpose, retention period, and who it will be shared with;

- The right of access: the right to access their personal data and be aware of and verify the lawfulness of the processing (see Related Guidance for further guidance relating to Subject Access Requests);

- The right to rectification: to have inaccurate personal data rectified or completed (if incomplete);

- The right to erasure: the right to have personal data erased (or 'the right to be forgotten'); this is not absolute, however, and will only occur in very limited circumstances in the University context;

- The right to restrict processing: the right to request restriction or suppression of their personal data; again, this only applies in certain circumstances and you are still permitted to store the data;

- The right to data portability: the right to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability;

- The right to object: to processing based on legitimate interests, direct marketing, and processing for purposes of scientific/historical research and statistics – unless certain conditions are met; and

- Rights in relation to automated decision making and profiling.

4.5 **International Transfers**

4.5.1 Under the GDPR, there is a general prohibition on transfers of personal data by both controllers and processors to jurisdictions outside the European Economic Area (EEA) unless the conditions for transfer are met. The University must ensure that adequate or equivalent controls are in place and all requirements of the GDPR are complied with in respect of any transfer. The DPO should be made aware of any transfer of personal data outside of the EEA. (Further information can be found in the University's Related Guidance).

4.6 **ICO Registration and Information Asset Register**

4.6.1 As the University is a data controller, it is registered with the Information Commissioner's Office. The register entry provides an overview of the personal

data being processed by the University and the reasons and purposes for processing the data. A link to the University's ICO register is provided at the end of this policy document.

4.6.2 As part of its GDPR compliance activities, and as a way of ensuring a record of data processed and the associated purposes are recorded formally internally, the University has established an Information Asset Register.

4.7 **Data Protection Impact Assessments**

4.7.1 Under the GDPR, organisations are required to complete a Data Protection Impact Assessment (DPIA) for new projects/processes or for types of processing that are likely to result in a high risk to the rights of data subjects.

4.7.2 DPIAs should include consultation with the DPO, and other relevant individuals or experts where appropriate.

4.7.3 A DPIA should include:

- A description of the nature, scope, context, and purposes of data processing;
- Assess necessity, proportionality, and compliance measures;
- Identify and assess risks to individuals; and
- Identify any additional measures to mitigate those risks.

4.8 **Data Breaches**

4.8.1 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.

4.8.2 All personal data breaches must be reported to the DPO / Information Management team **immediately**.

4.8.3 Under the GDPR, all organisations are required to report certain types of personal data breaches to the Information Commissioner's Office within 72 hours, where feasible. The DPO will categorise the breach and make a decision about whether or not the breach should be reported to the ICO, and advise on any further actions that need to be taken (e.g. informing the individuals affected, where required).

4.8.4 A link to the University's breach reporting process and contact details are provided at the end of this policy document.

5. BREACH OF THIS POLICY

5.1 Where there is deliberate misconduct or behaviour amounting to a wilful breach of this Data Protection policy, or gross negligence causing a breach of the policy, the matter may be considered under the University's Disciplinary Procedure under Regulation 31.

6. LEGISLATION AND GOOD PRACTICE

6.1 The details of the GDPR can be found at the following link: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

6.2 The details of the Data Protection Act 2018 can be found at the following link: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

6.3 The Information Commissioner's Office provides guidance and a guide to the GDPR on their website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Review / Contacts / References	
Policy title:	Data Protection Policy
Date approved:	8 May 2018
Approving body:	University Executive Group Information Governance Committee
Last review date:	June 2019
Revision history:	Version 1: May 2018 Version 2: June 2019
Next review date:	June 2020 (annually)
Related internal policies, procedures, guidance: University of Sussex's ICO register entry https://ico.org.uk/ESDWebPages/Entry/Z6428144 Data Protection Webpages http://www.sussex.ac.uk/ogs/policies/information/dpa Information Security Policies https://www.sussex.ac.uk/infosec/policies University Privacy Notice http://www.sussex.ac.uk/about/website/privacy Master Records Retention Schedule http://www.sussex.ac.uk/ogs/policies/information/recordsmanagementguidance *(currently under review)* Data Breach Reporting Process http://www.sussex.ac.uk/ogs/policies/information/dpa/reportingdatabreaches Rights of Individuals & Subject Access Requests http://www.sussex.ac.uk/ogs/policies/information/dpa/rightsofindividuals Data Protection Officer http://www.sussex.ac.uk/ogs/policies/information/dpa/dataprotectionofficer Lawful Bases for Processing Personal Data http://www.sussex.ac.uk/ogs/policies/information/dpa/processingdata Information Asset Owners http://www.sussex.ac.uk/ogs/policies/information/gdpr/iaos	
Policy owner:	Information Management Team
Lead contact / author:	Karen Blackman, Information Manager Alexandra Elliott, Head of Information Management and Compliance