UNIVERSITY OF SUSSEX

General Counsel, Governance and Compliance

DATA PROTECTION POLICY

1. OVERVIEW AND PURPOSE

1.1 Data protection is about the fair and appropriate use of information relating to identifiable individuals, and it is a crucial part of building trust between people and organisations.

1.2 The University has a duty to comply with the principles and requirements of data protection legislation[1] when processing personal data[2]. Failure to do so could have significant financial, regulatory and reputational impacts for the University.

1.3 The purpose of this policy is to:

- Outline the data protection principles and define key terms;
- Detail the rights of data subjects;
- Lay out the University's obligations under data protection legislation; and
- Make clear the specific responsibilities for compliance within the University.

2. SCOPE

2.1 This policy applies to, and must be adhered to, by 'all staff' processing personal data for the University.

2.2 For the purposes of this policy, 'all staff' includes the following, whether remunerated or not:

- Senior managers, officers, and directors;
- Employees (whether permanent, fixed-term, temporary, or casual);
- Contract, seconded, and agency staff;
- Volunteers, apprentices, and interns; and
- Others associated with (i.e. performing services for or on behalf of) the University (for example, agents and consultants).

2.3 Except where a student is also 'staff' of the University, or processing personal data as a part of the University's functions (e.g. as part of research work), this policy does not apply

[1] Data protection legislation is any applicable legislation relating to the processing of personal data and includes the Data Protection Act 2018, the UK General Data Protection Regulation and, in certain circumstances, the EU General Data Protection Regulation 2016/679.

[2] Personal data means any information relating to an identified or identifiable living individual and processing includes collecting, recording, storing, using, analysing, combining, disclosing or deleting personal data.

directly to students. However, students should be aware of their rights as data subjects and the University's responsibilities with regard to their own personal data.

2.4 Third parties who process personal data for the University also have obligations under data protection legislation that those engaging them must be aware of (see '4.4 Data Processors' for further details).

3. RESPONSIBILITIES

3.1 All Staff

3.1.1 All staff are responsible for familiarising themselves with this policy and must ensure that they adhere to the data protection principles when processing personal data as part of their work for the University.

3.1.2 All staff should be aware of their responsibilities and should consult and follow guidance and advice issued by the University's Data Protection Officer (see '4.9 Guidance and Advice') in relation to compliance with data protection legislation.

3.1.3 All staff are required to complete data protection-related training as required by the University.

3.1.4 All staff are responsible for ensuring they report any personal data breaches they become aware of to the Data Protection Officer immediately via the University's personal data breach reporting process(es).

3.2 Heads of Schools and Professional Services Directors

3.2.1 Heads of Schools and Professional Services Directors are responsible for ensuring that staff in their area are aware of this policy and their responsibilities (outlined in section 3.1), including completion of mandatory University data protection training.

3.2.2 Heads of Schools and Professional Services Directors are expected to encourage and promote a culture of compliance with regard to data protection within their School or Division.

3.2.3 Heads of Schools and Professional Services Directors should work in conjunction with the relevant Information Asset Owner(s) within their School or Division to identify, record, and manage data risks.

3.3 University Executive Group (UEG)

3.3.1 UEG is responsible for supporting and driving the broader data protection and information security agenda at the University, as well as providing assurance that effective best practice mechanisms are in place across the University.

3.3.2 As such, within the context of data protection, UEG is responsible for:

- Reviewing, contributing to, and approving data protection-related strategies and policies;

- Ensuring provision of resource to deliver approved strategies, and monitoring performance;

- Reviewing the operational status of data protection compliance across the University and acting as a point of escalation for related issues;

- Reviewing regulatory obligations and having oversight of legislative requirements in relation to the data protection and related legislation; and

- Ensuring that the Data Protection Officer has appropriate levels of autonomy and adequate support and resources in order to enable them to undertake their role effectively and to fulfil the requirements of the role.

3.4 **The Data Protection Officer (DPO)**

3.4.1 The DPO is responsible for monitoring internal compliance with data protection legislation, 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) (including reporting personal data breaches on behalf of the University).

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

3.5.1 The Senior Information Risk Owner (SIRO) is a member of the senior management team who is accountable for information risk across the University.

3.5.2 The SIRO is responsible for leading a culture of good information management, and for providing assurance to senior management that information risk is being managed appropriately and effectively across the organisation.

3.6 **Information Asset Owners (IAOs)**

3.6.1 The IAOs work with the DPO and Information Management team to keep the University's Information Asset Register up to date and should, within their area:

- Have an awareness of any processing activities, as well as an understanding of the repositories that hold personal data;

- Understand where and when data is shared with third parties, and whether that is covered by contractual or data sharing arrangements;

- Have a broad understanding of privacy issues and when there may be a need to conduct a Data Protection Impact Assessment (DPIA);

- Ensure that the Information Asset Register reflects all information assets and how personal data is process; and

- Understand any processing issues with existing or new activities and identifying where there are compliance issues to address.

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

4. POLICY DETAILS

4.1 Data Protection Principles

4.1.1 Data protection legislation outlines the following principles that must be adhered to when processing personal data:

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[3] is responsible for, and must be able to demonstrate compliance with, the above ('accountability').

4.2 Accountability

4.2.1 The University, as a data controller, is responsible for ensuring that the appropriate technical and organisational measures are put in place to meet the data protection principles, including:

- adopting and implementing data protection policies and appropriate security measures;

[3]A data controller determines the purposes and means of the processing of personal data and has overall responsibility for compliance, including compliance of its processor(s). Processors act on behalf of, and on the instructions of, the data controller.

- ensuring that procedures and process reflect data protection requirements, and reviewing these as required;

- 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 personal data breaches and reporting breaches to the Information Commissioner's Office when required;

- carrying out Data Protection Impact Assessments for processing activities that are likely to result in a risk to the interests and rights of data subjects;

- Creating a culture that values and prioritises privacy issues; and

- Ensuring staff are trained in data protection and aware of their responsibilities.

4.3 **Personal Data & Processing**

4.3.1 The University must have a lawful basis for processing personal data, and the available lawful bases under data protection legislation are outlined below:

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

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

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

- Public Task[4]: the processing is necessary in order to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

- Legitimate Interests: the processing is necessary for the University's 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 to processing carried out as part of the University's public task).

- Consent: the individual has given fully informed, explicit consent for the University to process their personal data for a specific purpose.

[4] The University's public task is set out in our Royal Charter – "*to advance learning and knowledge by teaching and research to the benefit of the wider community*".

4.3.2 The legal basis for processing should always be determined before the data is processed and documented. The University's privacy notice broadly outlines the legal bases for processing carried out as part of the University's standard functions.

4.3.3 In order to lawfully process special category data[5] and criminal offence data, additional conditions must be met.

4.4 **Data Processors**

4.4.1 Whenever a third party is used to process personal data for the University, staff must ensure that the appropriate legal / contractual arrangements are in place and the University must be assured that the processor can demonstrate compliance with data protection legislation requirements. Arrangements with processors should be approved by the DPO.

4.4.2 Data protection legislation places specific legal obligations on data processors. Data processors have legal liability if responsible for a data breach, although the data controller still has overall responsibility for compliance.

4.5 **Data Subject Rights**

4.5.1 Data protection legislation provides the following rights for data subjects:

- The right to be informed: to be informed about the collection and use of their personal data;
- The right of access: to access and receive copies of their personal data;
- The right to rectification: to have inaccurate personal data rectified or completed (if incomplete);
- The right to erasure (or 'to be forgotten'): to ask for personal data to be erased; this is not absolute, however, and will only occur in limited circumstances in the University context;
- The right to restrict processing: to request restriction or suppression of their personal data; again, this only applies in certain circumstances and storage of the data is still permitted;
- The right to data portability: to obtain and reuse their personal data for their own purposes across different services;
- The right to object: to object to the processing of their personal data in certain circumstances; and
- Rights in relation to automated decision making and profiling.

[5] Special category data refers to personal data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, an individual's sex life or sexual orientation, as well as genetic and biometric data.

4.5.2 The University must have appropriate processes in place to comply with data subject requests, and within the associated statutory timescale. The University's DPO should be contacted whenever a data subject request is received.

4.6 International Transfers

4.6.1 Personal data must not be transferred outside of the United Kingdom unless appropriate safeguards are in place to ensure an equivalent level of data protection. Generally, such safeguards will be limited to the following:

- The United Kingdom has made a decision that the third country ensures an adequate level of protection (an adequacy decision); or
- An appropriate transfer mechanism is in place, such as the use of an International Data Transfer Agreement (IDTA).

4.6.2 Where the transfer is to a country without an adequacy decision, advice should be sought from the DPO at the very earliest opportunity.

4.7 Data Protection Impact Assessments

4.7.1 Under data protection legislation, organisations are required to complete a Data Protection Impact Assessment (DPIA) for types of processing that are likely to result in a high risk to the rights and freedoms of data subjects.

4.7.2 DPIAs should include consultation with the DPO, as well as other relevant individuals or stakeholders 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, who will decide whether they are reportable to the Information Commissioner's Office or to data subjects. The DPO will also advise on action that is required internally and provide guidance to assist with mitigating risk of future breaches.

4.8.3 The University must report certain types of personal data breaches to the Information Commissioner's Office within 72 hours of the institution becoming aware of the breach. As such, breaches should always be reported to the DPO **immediately**.

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

4.9 **Guidance and Advice**

4.9.1 The DPO publishes guidance and advice in relation to a number of data protection compliance matters – including the processing of special category and criminal convictions data, handling data subject requests, international data transfers, carrying out Data Protection Impact Assessments, and reporting data breaches – on the data protection webpages, linked at the end of this policy.

4.9.2 Guidance and advice should always be sought from the DPO if staff are unsure how to proceed with any data protection-related matters.

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

6.2 The Information Commissioner's Office guidance on basic data protection concepts provides helpful definitions of key terms and concepts: https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/some-basic-concepts/

6.3 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

Review / Contacts / References	
Policy title:	Data Protection Policy
Date approved:	23 May 2022
Approving body:	University Executive Group
Last review date:	April/May 2022 February 2021 June 2019
Revision history:	Version 4: May 2022 Version 3: February 2021 Version 2: June 2019 Version 1: May 2018
Next review date:	April 2025 (or sooner, as required)
Related internal policies, procedures, guidance: Data Protection Webpages http://www.sussex.ac.uk/ogs/policies/information/dpa Data Breach Reporting Process http://www.sussex.ac.uk/ogs/policies/information/dpa/reportingdatabreaches University Privacy Notice http://www.sussex.ac.uk/about/website/privacy Information Asset Owners & Information Asset Register http://www.sussex.ac.uk/ogs/policies/information/dpa/iaos Information Security Policies https://www.sussex.ac.uk/infosec/policies Records Management Guidance https://www.sussex.ac.uk/ogs/information-management/records-management	
Policy owner:	Information Management Team
Lead contact / author:	Information Manager (Karen Blackman) Head of Information Management and Compliance (Data Protection Officer)