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

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

3.6.2

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

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

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: