DATA PROTECTION POLICY V4.2

05/05/2023

Elaine Grant, Data Protection Officer

Version control and history

Title	Description	Author	Approval
University Data Protection Policy	1st version of the University's Data Protection Policy in relation to 1998 legislation.	Craig Williamson	University Court. October 2001
Data Protection Policy v2.0	Major redraft of the above policy.	Elaine Forbes	Information Strategy Committee 25 October 2012
Data Protection Policy v2.1	Minor amendments to update outdated links in section 10.	Elaine Grant	Updated 06 January 2017. Approval not required due to minor nature of amendments.
Data Protection Policy v2.2	Minor amendment to refer to University Secretary and Compliance Officer	Elaine Grant	Update 13 December 2017. Approval not required due to minor nature of amendments
Data Protection Policy v3.0	Major redraft to ensure compliance with General Data Protection Regulation	Elaine Grant	Digital Campus Sub-Committee 23 May 2018
Data Protection Policy v3.1	Point 4.3 included Name of v3.0 changed in this front table from 'Data Protection and Privacy Policy v3.0' to 'Data Protection Policy v3.0'	Elaine Grant	Update 19/03/2019 Approval not required due to minor nature of amendments
Data Protection Policy v4.0	Major redraft	Elaine Grant	Information Strategy Committee 26/03/2020
Data Protection Policy v4.1	Minor amendment to reflect change in legislative references in 1.4. Hyperlink to data breach (8.6) reporting updated.	Elaine Grant	Update 26/11/2021 Approval not required due to minor nature of amendments

Data Protection Policy v4.2	Update role and responsibilities to refer to University Compliance Officer (instead of University Secretary and Compliance Officer)	Elaine Grant	Update 05/05/2023 Approval not required due to minor nature of amendments

Contents

1. Introduction

1.1 'Personal data' is information which relates to an identifiable living individual, who can be directly or indirectly identified from the information.

1.2 'Special category personal data' is personal data relating to: racial or ethnic origin; political opinions; religious of philosophical beliefs; trade union membership; genetic data; biometric data (where used for identification purposes); health; sex life; and sexual orientation.

1.3 All personal data must be 'processed' (e.g. collected, recorded, organised, stored, adapted, retrieved, used, disseminated, erased, or destroyed) in accordance with applicable data protection legislation.

1.4 Applicable data protection legislation is the United Kingdom General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 (DPA). This policy continues to apply if the legislation is amended in future.

1.5 This policy continues to apply until it is updated. In the event of legislative change that results in inconsistencies with this policy, legislative requirements take precedence until such time as the policy is reviewed.

2. Purpose

2.1 This policy sets out the University's commitment to comply with data protection legislation, whether it is acting as a data controller[1] or a data processor[2].

2.2 It sets out the responsibilities of the University and those who process personal data on its behalf.

2.3 This policy and associated policies, procedures and guidance form a framework within which those processing personal data should operate. This framework will assist the University in complying with its legal obligations.

3. Scope and status

3.1 The policy applies to all University staff, students and others, where they are processing personal data for University purposes, whether the University is acting as a data controller or processor.

3.2 The policy applies to all personal data processed by or on behalf of the University, irrespective of who created the data, its format, or where it is held.

[1] "Data controller" or "controller" means a person or organisation who (either alone or jointly with others) determines the purposes and means of processing personal data.
[2] A "data processor" or "processor" is responsible for processing personal data on behalf of a controller (but does not refer to the employees of a controller).

3.3 The University is required to have an Appropriate Policy Document (APD) in place when relying on certain substantial public interest conditions as set out in Schedule 1 of the Data Protection Act 2018. The APD is a separate, but related policy, and can be found on our website.

4. Data Protection Principles

4.1 The GDPR sets out six principles governing the use of personal information, which must be adhered to when processing personal data:

a) lawfulness, fairness and transparency;
b) purpose limitation;
c) data minimisation;
d) accuracy;
e) storage limitation; and
f) integrity and confidentiality (security).

4.2 In addition, organisations must be able to demonstrate compliance with these principles. This is known as the 'accountability principle'.

4.3 Whenever the University is processing personal data, it must do so in compliance with all of the principles, as set out in 4.1 and 4.2.

5. Roles and Responsibilities

5.1 The University Compliance Officer has overall institutional responsibility for compliance with this policy and the legislation.

5.2 Chief Officers, Deans and Directors (with responsibility for non-academic departments) are ultimately responsible for ensuring that their areas are compliant with this policy and that any Data Protection Audits, as issued by/on behalf of the Data Protection Officer, are completed.

5.3 Heads of School/Department (academic and service) have direct responsibility for ensuring that: their area complies with the legislation; that data protection issues are given due consideration; that any policies and procedures to raise awareness of DP obligations/implications for staff are implemented and supported; that a DP Contact is appointed; and that any Data Protection Audits, as issued by/on behalf of the Data Protection Officer, are completed.

5.4 The role and duties of the Data Protection Officer (DPO) are set out in legislation. The University's DPO is responsible for: the production and maintenance of this policy; assisting the University in monitoring internal compliance; informing, advising and training staff on data protection obligations; and acting as a contact point for data subjects and the supervisory authority, the Information Commissioner's Office (ICO).

5.5 The Information Governance Unit (IGU), under the direction of the DPO, provides advice and guidance in relation to data protection matters throughout the University and is responsible for overseeing the handling of requests in relation to data subjects' rights.

The IGU will manage regular University-wide departmental audits of DP.

5.6 A departmental Data Protection Contact (DP Contact) should be appointed for every business area/dept. to: promote awareness; advise colleagues; disseminate information; assist the IGU in responding to requests from data subjects; and assist their department in completing any DP Audits. It is the responsibility of the Head of Department/Director to appoint a DP Contact. If no DP Contact is appointed, the Head of Department/Director assumes the role. The IGU must be notified of the name of the DP Contact and kept informed of any changes.

5.7 All staff and workers, including those covered by ongoing and fixed term employment contracts, assignments or visiting and honorary appointments ('staff'), must comply with this policy and associated guidance. Staff must ensure that they understand the requirements of data protection legislation. Training, resources, advice and guidance is available via the IGU. Specifically, staff must ensure that:

- they have sufficient knowledge of data protection, including undertaking training as required;
- they follow relevant advice, guidance and tools/methods relating to the processing of personal data, either that provided by the ICO, IGU, or as set out in relevant University policies, procedures or processes;
- they process personal data only as necessary for their contractual duties and/or University role;
- they can recognise a potential or actual incident/security breach relating to personal data;
- they are aware of and understand the internal reporting requirements relating to data security incidents/breaches (see 8.6) and cooperate with any subsequent actions required to contain, mitigate and/or investigate the breach;
- they can recognise a request from a data subject to exercise their rights under DP legislation, deal with any such requests in a timely manner, and co-operate with the fulfilment of such requests, as required; and
- they only delete, copy or remove personal data when leaving the University as agreed with their line manager and as appropriate.

5.8 Where staff are responsible for students who are processing personal data as part of their research studies, the staff member must make sure that they direct the student to this policy and to any other resources or guidance required to ensure they comply with the legislation.

5.9 Staff are responsible for ensuring that their own personal information which they supply to the University is accurate. Where there is any change to their personal information they are required to inform the University of any updates/changes or update this information themselves via University systems.

5.10 Where the University engages or appoints a third party to process personal data on its behalf e.g. consultants, contractors etc., those organisations/individuals must be made aware of this policy and their obligations. The University staff responsible for the activity must ensure that the third parties are made aware of their obligations and, where

appropriate, that agreements are in place to safeguard personal data, e.g. data processing agreements.

6. Responsibilities of Third Parties Working on Behalf of the University

6.1 The University is responsible for the processing of personal data by third party companies or individuals working on its behalf. Appropriate written agreements must be in place, prior to processing, where required.

6.2 Third parties are required to comply with this policy and, in particular, must ensure that they understand the requirements of data protection legislation.

7. Responsibilities of Students

7.1 All students processing personal data on behalf of the University are required to comply with this policy and any other relevant procedures/guidance.

7.2 Students who are considering processing personal data as part of their studies should obtain approval from the appropriate member of academic staff before processing takes place.

7.3 Students are responsible for ensuring that their own personal information which they supply to the University is accurate. Where there is any change to their personal information they are required to inform the University of any updates/changes or update this information themselves via University systems.

8. Compliance with the legislation

8.1 All those who process personal data on behalf of the University must ensure that they do so in compliance with applicable legislation. In addition to the information set out above, this includes being aware of the points below and taking any steps necessary to comply.

8.2 The University is committed to adopting a culture of 'data protection by design and default'. This includes:

- considering data protection issues as part of the design and implementation of systems, services, products and business practices;
- ensuring adequate technical and organisational measures are in place to ensure the security of data;
- having robust data security incident reporting and management processes;
- embedding data protection impact assessments (DPIAs) in relevant processes to ensure mandatory requirements to undertake DPIAs for high risk processing are met, as well as where the University deems it appropriate and helpful to do so, to assess privacy risks;
- ensuring that we have data processing agreements in place with our processors;
- data sharing is documented and agreements in place, where required; and

- ensuring that our systems and technologies are capable of adequately protecting personal data.

8.3 All individuals have rights in relation to their personal data. The University:

- is committed to upholding the rights of individuals; and
- will comply with individuals' requests in relation to their personal data where legally required to do so, and otherwise in so far as we are able.

8.4 We must comply with the 'storage limitation' principle and ensure that we do not retain data for longer than is required. Records Management policies, procedures and guidance should be adhered to.

8.5 University policies and procedures around Information Security, cyber security and confidential waste are intrinsically linked to data protection, in order to comply with the 'integrity and confidentiality' principle. All those who process personal data on behalf of the University should familiarise themselves with associated policies and procedures and undertake any relevant training.

8.6 The University has personal data security incident reporting and management procedures, which all staff are required to follow.

8.7 It is recommended that all staff undertake data protection training. The IGU provide training resources that are accessible to all staff.

9. Impact of Non-compliance

9.1 Failure to comply with the policy can lead to:

- damage and distress to the individuals whose personal data has not been managed appropriately;
- damage to the University's reputation and its relationship with stakeholders;
- significant legal and financial consequences; the Information Commissioner's Office (ICO) which enforces data protection legislation in the UK can investigate and take enforcement action in case of non-compliance. This can include substantial fines.

9.2 Any individual who is found to have failed to comply with the policy may be in breach of their conditions of employment and therefore subject to disciplinary action.

9.3 Failures to comply with the policy (and the legislation) which may result in disciplinary action include (but are not limited to): knowingly or recklessly obtaining, disclosing (or procuring the disclosure of), or retaining personal data, without the consent of the controller; knowingly or recklessly re-identifying de-identified personal data, without the consent of the controller; and altering, deleting, erasing or otherwise preventing the disclosure of personal data to a data subject who has made a subject access request (and who would have been entitled to receive information in response to that request).

9.4 It should be noted that the actions listed in 9.3 are also criminal offences, as set out in the DPA, and individuals can be prosecuted by the relevant authorities. Nothing set out elsewhere in this policy waives any personal liability for individual criminal offences under data protection law.

10. Review

10.1 This policy will be subject to review by the appropriate University body every three years, or as otherwise required.

10.2 Minor amendments, e.g. typographical errors or updates to legislative references may be made by the DPO without formal approval.

10.3 Any significant amendments will require the policy to be submitted for approval via the appropriate University process.