UNIVERSITY OF ABERDEEN

DATA PROTECTION POLICY

1. Purpose

This policy sets out the principles, responsibilities and obligations for managing personal data within the University. The policy is designed to ensure the University complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) when processing personal data for its teaching, research, administrative and other legitimate activities.

2. Scope

This policy applies to the processing of personal data as follows:

- It applies to processing activities performed on personal data on behalf of the University in its role either as the controller of personal data or as the processor of personal data for another controller. For definitions of 'personal data', 'processing', 'controller', 'processor' and other key terms, see the Glossary at the end of this policy.
- It applies to personal data held in any format, including on paper and in digital formats.
- It applies to all members of staff employed by the University, and to persons with honorary staff status given access to University information or IT facilities ('staff').
- It applies to registered students when they process personal data in connection with their academic studies or research at the University other than under the supervision or instruction of a University member of staff. The policy is likely to apply to registered students only in exceptional circumstances.

3. Roles and responsibilities

The roles that carry responsibilities under this policy are as follows:

- Heads of Schools and Directors of Professional Services are responsible for the operation of this policy within their respective areas of responsibility and for promoting compliant data protection practices. Heads of School and Directors are supported in their schools / directorates by nominated information champions.
- Staff (and, where relevant, registered students) are responsible for acting in accordance with this policy and with any instructions for handling personal data they are given by the University. Staff are also responsible for ensuring that any processing of personal data they direct or require registered students to undertake for the purposes of academic studies or research complies with this policy.
- The University Data Protection Officer (DPO) is the designated data protection officer for the University, and shall provide support, training and guidance to Heads of School and Directors, information champions and staff, assisted by other members of the Information Governance team. The DPO shall perform the tasks and duties of the data protection officer specified in the UK GDPR.

- Members of senior management are responsible for involving the DPO in all significant data protection issues affecting the University.
- The Director of Digital and Information Services has delegated responsibility for establishing and maintaining the University of Aberdeen's ISMS to ensure the availability, integrity and confidentiality of the University of Aberdeen's information. The Director of Digital and Information Services will lead on the definition and implementation of the University of Aberdeen's information security and governance arrangements and make judgement calls when situations arise that are not covered by the current information security management framework.
- The Information Governance Committee has executive responsibility for data protection compliance within the University, and for taking steps to address risks and issues of concern.
- The Information Risk Working Group is responsible for reviewing information governance and security risk and advising on risk treatment efforts and consistent implementation of this policy.

4. Standards and procedures for processing personal data

Data protection principles

Governance roles

Lawful bases for processing personal data

Requirements for special categories of personal data and criminal offence data

Requirements for processing personal data of vulnerable people

Purposes for processing personal data

Technical, organisational and security measures to manage data protection risks

Data processing arrangements – the University as controller

Data processing arrangements – the University as processor

Data sharing arrangements

Disclosures of personal data

International transfers of personal data

Personal data breaches

Data subjects' rights

Data subject rights – requests to the University

Data subject rights - the right to be informed

Procedures, training and guidance

Compliance and monitoring

Data protection principles

4.1 The UK GDPR sets out the following seven governing principles.

Principle 1: **Lawfulness, fairness, transparency**

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

Principle 2: **Purpose limitation**

Personal data shall be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Principle 3: **Data minimisation**

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Principle 4: **Accuracy**

Personal data shall be 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.

Principle 5: **Storage limitation**

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed.

Principle 6: **Integrity and confidentiality**

Personal data shall be 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.

Principle 7: **Accountability**

The University shall be responsible for, and be able to demonstrate compliance with, the UK GDPR.

Governance roles

4.2 The University is responsible for complying with the data protection principles, and the underpinning obligations in data protection legislation, when processing personal data as a controller for its own purposes such as in teaching, research and carrying out administrative functions.

4.3 External organisations involved in a data processing activity with or for the University also bear responsibility for compliance under data protection legislation. Those organisations may qualify as a controller, a joint controller or a processor depending on their role in deciding why and how personal data are processed in that data processing activity.

4.4 Where the University processes personal data solely for the purposes of an external organisation, the primary responsibility for complying with data protection legislation lies with the external organisation as the controller. In those circumstances, the University functions as a processor and is responsible for the limited obligations placed on processors under data protection legislation.

4.5 Determining whether the University and external organisations qualify as controllers or processors, and determining whether controllers are independently or jointly responsible for data protection compliance, can be complex. Guidance on the factors that should be taken into account when deciding data protection roles is available from the DPO.

Lawful bases for processing personal data

4.6 The UK GDPR requires that personal data shall be processed only if one or more of the following conditions apply. (Note that the conditions are not ranked in order of importance or relevance to the University.)

Article 6(1)(a): **Consent**

The data subject has given consent to the processing of their personal data for one or more specific purposes.

Article 6(1)(b): **Contract**

Processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract.

Article 6(1)(c): **Legal obligation**

Processing is necessary for compliance with a legal obligation to which the controller is subject.

Article 6(1)(d): **Vital interests**

Processing is necessary to protect the vital interests of the data subject or of another natural person.

Article 6(1)(e): **Public task**

Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

Article 6(1)(f): **Legitimate interests**

Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

For guidance on the scope of each of the six conditions, see the StaffNet Data Protection page on Lawful Basis.

4.7 A record of the conditions on which the University relies to process personal data shall be maintained by the DPO. Heads of School / Directors shall assist the DPO to maintain

an accurate and up-to-date record of the lawful basis for data processing activities in their area of responsibility.

4.8 Routine processing of the personal data of applicants to study, students, alumni, applicant for posts, staff, former staff and research participants as part of the University's core teaching, research and administrative tasks is likely to be lawful under conditions (b), (c) and/or (e). Many of the University's data processing activities will be covered by these conditions.

4.9 Where no contractual relationship exists between the University and the data subject, and there is no identified statutory or regulatory power or obligation to process personal data, staff shall ensure there is a lawful basis under data protection legislation for their processing of personal data. Guidance on the lawful basis in particular circumstances is available from the DPO.

4.10 In cases where the University relies on consent of the data subject to process personal data, condition (a), staff shall keep an appropriate record of consent. The UK GDPR sets a high standard for obtaining, recording and refreshing consent. For guidance on the requirements, see the StaffNet Data Protection page on consent. DPO advice is strongly recommended before embarking on new data processing activities based on this condition.

4.11 The scope of the legitimate interests condition, condition (f) is limited to data processing activities that do not form part of the University's core teaching, research and administrative tasks. In cases where this condition will be relied on to provide the lawful basis for processing, users shall undertake a 'legitimate interests assessment' before commencing any new data processing activities. Any legitimate interests assessment shall involve consultation with the DPO.

Requirements for special categories of personal data and criminal offence data

4.12 The UK GDPR and the DPA prohibit any processing of special categories of personal data or criminal offence data unless there is a relevant exemption for the activity. An exemption is required in addition to a lawful basis for processing.

4.13 The following types of personal data are classified as 'special categories' :

- Personal data revealing a person's racial or ethnic origin
- Personal data revealing a person's political opinions
- Personal data revealing a person's religious or philosophical beliefs
- Personal data revealing a person's trade union membership
- Genetic data (see the Glossary at the end of this policy)
- Biometric data processed for the purpose of uniquely identifying a person (see the Glossary at the end of this policy)
- Personal data concerning a person's health
- Personal data concerning a person's sex life

- Personal data concerning a person's sexual orientation

4.14 Criminal offence data is personal data that relates to criminal convictions and penalties, allegations of criminal activity, investigation of allegations and criminal justice proceedings. It covers personal data of victims and witnesses of crime as well as of offenders and suspects.

4.15 The exemptions permitting special categories of personal data to be processed are complex. Guidance on exemptions that may apply to new processing activities is available from the DPO.

4.16 A record of the additional conditions on which the University relies to process special categories of personal data shall be maintained by the DPO. Heads of School / Directors shall assist the DPO to maintain an accurate and up-to-date record of the conditions for relevant data processing activities in their area of responsibility.

4.17 The DPA requires any data processing involving special categories of personal data to be documented in an Appropriate Policy Document. The DPO shall maintain the Appropriate Policy Document(s) for the University's activities as a controller as part of the University's Record of Processing Activities.

Requirements for processing personal data of vulnerable people

4.18 People who are unable to easily consent to, or oppose, the way their personal data is processed because of a power imbalance between them and the University are considered vulnerable in data protection terms. Vulnerable people may include staff and students who are dependent on the University for their employment or academic award as well as children and ill people who lack the capacity to exercise their privacy rights knowingly.

4.19 Collection and use of personal data of vulnerable people is an indicator of a potential high-risk processing activity. Staff shall note the groups classed as vulnerable when assessing whether a data protection impact assessment is required for any new processing activity. See the section on Technical, organisational and security measures for further details on data protection impact assessments.

4.20 The Age Appropriate Design Code, also known as The Children's Code, specifies the design standards and privacy features for information society services likely to be accessed by children. Those services include websites, apps, search engines and social media platforms. Staff shall ensure that information society services offered by the University meet the requirements of the code wherever feasible. Guidance on the content and application of the code is available from the DPO.

Purposes for processing personal data

4.21 A record of the purposes for which the University processes personal data shall be maintained by the DPO in the University's Record of Processing Activities. Heads of School / Directors shall assist the DPO to maintain an accurate and up-to-date record for their area of responsibility.

4.22 The UK GDPR requires a 'compatibility assessment' to be carried out for any proposal to use existing personal data for an unrelated purpose, other than when the proposed processing is not based on the consent of the data subject or required by law. Users shall undertake and document a compatibility assessment when required to comply with this obligation. Any compatibility assessment shall involve consultation with the DPO.

Technical, organisational and security measures to manage data protection risks

4.23 The UK GDPR requires that new procedures and systems for processing personal data incorporate measures at the design stage to comply with the data protection principles. When developing new ways in which personal data is collected or used by the University, the member of staff responsible for the business process shall ensure the proposals comply with the data protection principles and incorporate any necessary safeguards to meet the standards set out in paragraph 4.1. Advice on appropriate measures is available from the Digital & Information Services Information Security team and Information Governance team.

4.24 The UK GDPR requires that a 'data protection impact assessment' (DPIA) is undertaken prior to undertaking any new processing activity that is likely to result in a high risk to individuals. There are certain processing activities that always meet this condition, known as mandatory circumstances. For the current list of circumstances, see the StaffNet Data Protection page on DPIAs. Staff shall carry out a DPIA when the proposed data processing activity meets one or more of the mandatory circumstances or when the proposal would otherwise be likely to result in a high risk to individuals.

4.25 The UK GDPR requires that any DPIA shall involve consultation with the DPO. Early contact with the DPO is recommended to guide staff through the process and advise on relevant risks. As a minimum, the DPO's comments shall be sought when the risk has been assessed and mitigation measures identified but before a decision is taken to proceed with the processing activity.

4.26 The Director of People shall ensure that the terms and conditions of employment require members of staff to process personal data only for the legitimate purposes of the University.

4.27 The UK GDPR requires the University to implement measures to ensure a level of security for personal data that is appropriate to the risk that processing poses to individuals. Security measures for University information, including personal data, are specified in the Information Security policy and procedures. The Director of Digital & Information Services shall ensure there are information security policies and procedures that will provide an appropriate level of protection for personal data.

4.28 Staff shall act in accordance with information security policies and procedures when processing personal data on behalf of the University to protect personal data against accidental or unlawful destruction, loss and alteration or unauthorised disclosure or access.

Data processing arrangements – the University as controller

4.29 A third party that processes personal data on behalf of the University is a 'processor' for the purposes of the UK GDPR. This could be a person or an organisation. University staff are not classed as processors, nor are third parties that process University personal data for their own purposes: see the section on Data Sharing for more details.

4.30 The UK GDPR requires that only those organisations or people that have provided sufficient guarantees about their security and data protection arrangements should be engaged as a processor. The UK GDPR also requires that an arrangement between the University and a processor is governed by a written agreement that incorporates specific safeguards. Staff shall follow the established supplier assessment processes to meet these two requirements. For guidance on engaging a processor, see the StaffNet Data Protection page on Supplier Assessment.

4.31 Staff responsible for the data processing arrangement shall ensure instructions to processors on how to handle personal data on behalf of the University are provided in writing and that significant instructions affecting the way that University personal data is handled are retained for the duration of the processing arrangement and in accordance with the University retention policy.

Data processing arrangements – the University as processor

4.32 The University may be engaged as the processor of personal data for the purposes of another controller. In these circumstances, the University is responsible to the controller for the way in which personal data is processed.

4.33 Staff shall ensure that the terms of any data processing contract covering their University activities as a processor of personal data for another controller are reasonable for the University and meet the statutory requirements. Guidance on the requirements is available on the StaffNet Data Protection pages.

4.34 Where the University is a processor on behalf of another controller, staff shall ensure that they act only on the documented instructions of the controller and adhere to the terms of the data processing contract. Staff shall notify the controller, after prior discussion with the DPO, if they believe that either any of the controller's instructions are unlawful or as soon as possible after becoming aware of a personal data breach of the controller's data.

Data sharing arrangements

4.35 An arrangement between the University and another organisation in which both parties determine why and how personal data will be processed is a 'data sharing' arrangement. In these circumstances, the University and the other organisation are both controllers for the purposes of the UK GDPR.

4.36 Where the University and the other organisation in a data sharing arrangement are independent controllers, staff shall consider documenting any systematic, routine disclosure of personal data in a data sharing agreement. Where the University and the

other organisation in a data sharing arrangement are joint controllers, staff must document the arrangement formally in a data sharing agreement.

4.37 A data sharing agreement involving personal data should document the parties involved, the purposes of the arrangement, the data to be shared, the lawful basis and any exemptions for special category of personal data or criminal offence data, the arrangements for complying with data subjects' rights and the operational procedures for sharing data, including any agreed security measures to protect the data. Further guidance is available on the StaffNet Data Protection page on data sharing.

Disclosures of personal data

4.38 Staff shall ensure any disclosure of personal data to a third party is fair and lawful and complies with the data protection principles (see paragraph 4.1). In particular, staff shall ensure that a secure method is used to transfer personal data to an external party. For guidance on methods of secure data transfer, see the StaffNet IT Services Collaboration page. The recipient's identity and address (including email address) should also be verified and checked before any internal or external transfer of personal data.

4.39 Staff shall retain a record of personal data disclosed to a third party in accordance with the University retention policy.

International transfers of personal data

4.40 The UK GDPR allows personal data to be transferred to countries outside the United Kingdom or to international organisations only when one of the conditions specified in the UK GDPR are met by the controller and the processor. Transfers may be made based on a country's adequacy, under an appropriate legal agreement with the recipient or in exceptional circumstances. See the StaffNet Data Protection page on Transferring Data Abroad for the list of countries deemed 'adequate', links to the model agreements and guidance on the exceptional circumstances.

4.41 Staff shall ensure that international transfers of personal data from their area of responsibility meet one of the conditions set out in Part V of the UK GDPR.

4.42 There is one authorised exception to this policy requirement. Transfers of student personal data to higher education partners based outside the United Kingdom as part of an international exchange programme are permitted where none of the UK GDPR safeguards can be agreed with the partner as long as the arrangement is subject to the checks agreed by the Information Governance Committee on 16 November 2019. Guidance on these checks is available from the DPO.

Personal data breaches

4.43 The UK GDPR classes a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data as a 'personal data breach'.

4.44 Staff shall notify the DPO or the IT Service Desk and, if appropriate, their Head of School / Director as soon as practicable after discovery of a personal data breach. Prompt notification is essential to meet the deadline for onward notification of breaches to the regulator and affected data subjects.

4.45 Heads of School / Directors shall ensure the circumstances of all personal data breaches reported in their area of responsibility are investigated, and a risk assessment carried out to determine whether to notify the regulator and affected data subjects. The DPO or a member of the Information Governance team shall be involved in the assessment or investigation of all personal data breaches.

4.46 If required, following the risk assessment, the DPO shall notify a personal data breach to the Information Commissioner within 72 hours of confirmation a breach has occurred. Heads of School / Directors shall ensure that individuals affected by a personal data breach are notified when required.

4.47 The Director of Research & Innovation shall ensure that research funding bodies and/or partners are notified of personal data breaches where required by the relevant contract.

4.48 The DPO shall maintain a record of personal data breaches on behalf of the University. Heads of School / Directors shall ensure information relating to the facts of the breach, its effects and remedial action taken are provided to the DPO or the Information Governance team where necessary to complete this record.

4.49 Any member of staff who is found to have inappropriately accessed or divulged confidential (including personal) information will be subject to investigation under the University's disciplinary procedure, which may result in dismissal and possible legal action. It is an offence under the Data Protection Act 2018 where an individual knowingly or recklessly obtains, discloses, procures, sells or offers for sale, personal data without the consent of the University, as controller.

Data subjects' rights

4.50 The UK GDPR provides the following rights to individuals whose personal data is processed by the University:

- The right to be informed about personal data being processed
- The right of access to personal data
- The right to rectification of inaccurate personal data
- The right to erasure of personal data
- The right to restriction of processing of personal data
- The right to portability of personal data provided in a structured, commonly used and machine-readable format

- The right to object to personal data being processed on the lawful basis of a public task or official authority, or on the legitimate interests of the University or a third party
- The right to object to personal data being processed for direct marketing purposes
- The right to object to personal data being processed for scientific research, historical research or statistical purposes
- The right not to be subject to a decision based solely on automated processing
- The right to withdraw consent to personal data being processed by the University
- The right to contact the DPO about all issues relating to processing of their personal data and the exercise of their rights

4.51 These subject rights are not absolute. The rights are applicable in certain conditions specified in the UK GDPR and are subject to various exemptions set out in the DPA. These conditions and exemptions ensure individuals' rights are balanced against data processing activities deemed to be in the public interest, including the conduct of examinations, the conduct of research and the provision of confidential references. The operation of these rights is complex. For guidance on their scope and application, see the StaffNet Data Protection page on Data Subject Rights. Advice may be sought from the DPO on any particular circumstances.

Data subject rights – requests to the University

4.52 The Information Governance team shall log, co-ordinate and respond to valid data subject requests from individuals made to or forwarded to them.

4.53 Heads of School / Directors shall ensure information held by their area of responsibility is provided to the Information Governance team when required for a data subject request, including information that may be exempt from disclosure.

4.54 Staff shall refer the following requests to the Information Governance team for action:

- Requests in which a data subject explicitly invokes their rights under the UK GDPR or the DPA
- Requests for access to all personal data relating to the data subject held by all schools and services in the University
- Requests for personal data where there are concerns around disclosure of the requested information.

4.55 Staff may respond directly to the following types of request:

- Requests for access to personal data that would be routinely provided by the school or service in the course of teaching, student support, staff employment, research participation or event management
- Requests for correction of personal data gathered and maintained in the course of teaching, student support, staff employment, research participation or event management

- Unsubscribe responses or objections to direct marketing
- Withdrawal of consent for processing in cases where the lawful basis for processing personal data is consent, and the withdrawal request is made to the team responsible for that business process.

Data subject rights - the right to be informed

4.56 The UK GDPR requires privacy information to be provided to data subjects in the following three circumstances, unless there is a relevant legal exemption:

- when collecting personal data directly from individuals;
- following receipt of individuals' personal data from a third party; and
- when processing their personal data for a new purpose.

4.57 The required privacy information includes the identity of the controller, the contact details of the DPO, the purposes and legal basis for processing, the recipients of the data, any intended international transfers and the retention period. The information must be presented in a concise, transparent, intelligible and easily-accessible form. There are some, limited exemptions from this requirement, notably provisions for research. For guidance on the requirements for privacy information, see the StaffNet Data Protection page on Providing Privacy Information.

4.58 The DPO shall maintain corporate-level privacy information on the University website, including notices for students, staff, alumni and other major classes of data subject. Staff shall direct data subjects to the corporate-level privacy information on the University website in any forms, systems or processes that capture personal data from those individuals for University purposes in order to meet the UK GDPR requirement that privacy information is provided at the point personal data is gathered.

4.59 The University may collect and use personal data about data subject who are not included in a corporate-level privacy notice. Examples include the collection of information about people involved in one-off events, and collaborative projects with other organisations. Where personal data is processed without a corporate-level privacy notice, the member of staff responsible for the activity shall ensure the privacy information required by UK GDPR is provided to the relevant data subjects. Advice on the scope of corporate-level privacy notices is available from the DPO.

Procedures, training and guidance

4.60 The DPO shall develop and maintain procedures designed to ensure the University complies with data protection legislation and to support this policy.

4.61 The DPO, supported by the Information Governance team, shall deliver training and provide advice to staff on all aspects of data protection compliance and good practice.

4.62 Annual Data Protection Training is mandatory for all staff in line with the University's Information Security and Data Protection Training Strategy. Heads of School/Directors are responsible for ensuring that all staff within their remit are trained appropriately.

Compliance and monitoring

4.63 The DPO shall monitor the University's compliance with data protection requirements and shall report to the Information Governance Committee on compliance with data protection legislation and on significant data protection issues.

4.64 The DPO shall act as the contact point between the University and the Information Commissioner for matters relating to data protection compliance.

5. Related policies

The Information Security policy and procedures set out how information (including personal data) shall be secured to protect it against the consequences of breaches of confidentiality, failures of integrity, or interruptions to its availability.

The Records Management policy sets out how records (containing personal data) shall be managed and retained to support University functions and to comply with legal and accountability requirements.

6. Review and Development

The policy will be updated by the DPO when the Information Governance Committee agrees changes to meet internal or external requirements.

The policy shall be reviewed fully on an annual basis by the DPO and the outcome, including any recommendations for amendment, shall be reported to the Information Governance Committee.

Glossary of data protection terms

Term	Definition
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a person, which allow or confirm the unique identification of that person, such as facial images or dactyloscopic data.
Consent	Any freely-given, specific, informed and unambiguous indication of a data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of his or her personal data.
Controller	A person, public authority or body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Criminal offence data	Personal data relating to criminal convictions and offences, or related security measures.
Data concerning health	Personal data related to the physical or mental health of a person, including the provision of health services, which reveal information about his or her health status.
Data sharing	The disclosure of data from one or more organisations to a third party organisation or organisation, or the sharing of data between difference parts of an organisation.
Data processing agreement	A document that sets out instructions to be followed by a processor when processing personal data on behalf of a controller
Data sharing agreement	A document that sets out a common set of rules to be adopted by controllers involved in a data sharing operation.
Data subject	The identified or identifiable living individual to whom personal data relates.
Direct marketing	The communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.
DPA 2018	The Data Protection Act 2018
DPIA	Data protection impact assessment
DPO	Data Protection Officer
Filing system	Any structured set of personal data which is accessible according to specific criteria, whether held by automated means or manually and whether centralised, decentralised or dispersed on a functional or geographical basis.

Genetic data	Personal data relating to the inherited or acquired genetic characteristics of a person which give unique information about the physiology or the health of that person and which result, in particular, from an analysis of a biological sample from the person in question.
ICO **Information Commissioner**	The supervisory authority for data protection legislation in the United Kingdom. The ICO's web address is www.ico.org.uk.
Identifiable person	A person 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 person.
Information society services	A service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. See Directive (EU) 2015/1535 for an indicative list of services excluded from this definition.
Joint controller	A person, public authority or body which, jointly with other controllers, determines the purposes and means of the processing of personal data.
PECR	The Privacy & Electronic Communications (EC Directive) Regulations 2003 - 2016
Personal data	Any information relating to an identified or identifiable living person.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
Processing	Any operation which is performed on personal data, 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.
Processor	A person, public authority or body which processes personal data on behalf of the controller.
Profiling	Any form of automated processing personal data consisting of the use of personal data to evaluate certain personal aspects relating to that person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement.
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is

	subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable person.
Special categories of personal data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data or biometric data when processed to identify a person; or data concerning a person's health, sex life or sexual orientation.
UK GDPR	The UK General Data Protection Regulation. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018.

Approval/Review History

Version	Date	Action
[1.0]	University Court, 25 May 2004	Approved
[2.0]	University Court, 28 June 2011	Updated
[2.1]	Data Protection Officer, March 2015	Minor updates
[2.2]	Data Protection Officer, April 2015	Minor updates
3.0	Operating Board, 6 March 2019	Approved
4.0	Information Governance Committee, 16 April 2020	Approved
5.0	Information Governance Committee, 2 March 2021	Approved
6.0	Information Governance Committee, 11 August 2021	Approved
7.0	Information Governance Committee, 6 April 2022	Approved
8.0	Information Governance Committee, 19 January 2023	Approved

Policy Metadata

Metadata element	Metadata
Title	Data Protection Policy
Author / Creator	Data Protection Officer
Owner	Data Protection Officer
Date published / approved	19 January 2023
Version	8.0
Reviewed	December 2022
Date of next review	April 2024
Audience	All staff, students, partners, suppliers and contractors who process personal data for or on behalf of the University
Related documents	Information Security Policy Records Management Policy
Subject / Description	The activities and responsibilities involved in complying with data protection legislation.
Document status	Policy
Equality Impact Assessment	N/A
Theme	Information Management
Keywords	Personal data, information, processing, compliance, subject access, retention, sharing, disclosure, research, privacy, direct marketing