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 compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) whilst enabling the use of personal data for teaching, research, administrative and other legitimate activities.

2. Scope

This policy and its supporting guidance applies to the processing of personal data as follows:

- The policy 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. The terms 'personal data', 'processing', 'controller' and 'processor' are defined in the glossary.

- The policy applies to personal data held in any format, including on paper and in digital formats.

- The policy 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').

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 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 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 GDPR.

- Members of senior management are responsible for involving the DPO in significant data protection issues affecting the University.

- 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.

4. Standards and procedures for processing personal data

Data protection principles

4.1 The GDPR establishes the following six principles for the way in which personal data should be handled.

(1) *Lawfulness, fairness, transparency*
Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

(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.

(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.

(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.

(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.

(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.

4.2 Staff shall comply with the six principles when processing personal data on behalf of the University, unless a valid exemption applies. Guidance on available exemptions is available on the StaffNet Data Protection pages, and advice on their application to particular circumstances is available from the DPO.

Lawful basis for processing personal data

4.3 The 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.) Guidance on the scope of each of the six conditions is available on the StaffNet Data Protection pages.

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

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

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

(4) Processing is necessary in order to protect the vital interests of the data subject or of another natural person.

(5) 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.

(6) 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.

4.4 A record of the condition(s) 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.

4.5 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 (2), (3) and/or (5). The majority of the University's data processing activities will be covered by these conditions.

4.6 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.

4.7 In cases where the consent of the data subject provides the University with the lawful basis for processing, condition (1), the member of staff responsible for the business process that collects the personal data shall ensure an appropriate record of consent is kept. The GDPR sets a high standard for obtaining, recording and refreshing consent. Guidance on the requirements for consent is available on the StaffNet Data Protection pages. DPO advice is strongly recommended before embarking on new data processing activities based on this condition.

4.8 The scope of the legitimate interests condition, condition (6) 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, staff shall undertake a 'legitimate interests assessment' before commencing any new data processing activities. Any legitimate interests assessment shall involve consultation with the DPO.

Special categories of personal data

4.9 The GDPR and the DPA classify the following types of personal data as 'special category' personal data:

- 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
- Biometric data processed for the purpose of uniquely identifying a person
- Personal data concerning a person's health
- Personal data concerning a person's sex life
- Personal data concerning a person's sexual orientation
- Personal data relating to the alleged commission of offences by a person
- Personal data relating to the proceedings for an offence committed or alleged to have been committed by a person

4.10 Special categories of personal data may be processed only under certain conditions. These conditions are additional to the lawful bases for processing personal data listed in paragraph 4.3. The conditions for processing special categories of personal data are complex. Guidance is available on the StaffNet Data Protection pages, and advice on conditions that may apply to particular circumstances is available from the DPO.

4.11 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.

4.12 The DPA requires any data processing involving special categories of personal data to be documented in an 'additional policy document'. A member of staff responsible for a business process in which special categories of personal data are used by the

University shall ensure there is an additional policy document that meets statutory requirements. Creation of any additional policy document shall involve consultation with the DPO. The DPO shall retain all additional policy documents as part of the University's Record of Processing Activities.

Purposes for processing personal data

4.13 A record of the purposes for which the University processes 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 data processing activities in their area of responsibility.

4.14 The 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. Staff 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

4.15 The 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.

4.16 The 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. Staff shall carry out a DPIA when the proposed data processing activity falls into one or more of the following categories:

- Profiling individuals on a systematic and extensive basis to make decisions about them
- Processing special category personal data on a large scale
- Monitoring publicly-accessible places systematically and on a large scale
- Using new technologies to process personal data, or apply existing technologies in a novel way
- Using profiling, making automated decisions or using special category data to decide on an individual's access to services, opportunities or benefits
- Profiling individuals on a large scale
- Processing biometric data
- Processing genetic data, other than in the provision of health care

- Combining, comparing or matching personal data in datasets from different sources
- Collecting personal data from a source other than the individual without providing the individual with privacy information
- Tracking individuals' online or offline location or behaviour
- Profiling children or targeting marketing or online services at children
- Processing personal data that might endanger the individual's physical health or safety in the event of a security breach

4.17 Guidance on the procedure for carrying out a DPIA is available on the StaffNet Data Protection pages. The GDPR requires that any DPIA shall involve consultation with the DPO. Early contact with the DPO is recommended. 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.

4.18 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.

4.19 The 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. 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.

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

<u>Data processing arrangements – the University as controller</u>

4.21 A person or organisation that processes personal data on behalf of the University is a 'processor' for the purposes of the GDPR.

4.22 The 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 GDPR also requires that an arrangement between the University and a processor is governed by a written agreement that meets certain criteria laid down in the GDPR. Staff shall follow the supplier assessment and procurement processes established to meet these two requirements. Guidance on the requirements and procedures is available on the StaffNet Data Protection pages.

4.23 Members of staff responsible for the data processing arrangement shall ensure instructions to processors on how to handle personal data on behalf of the University 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

4.24 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.

4.25 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.

4.26 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 if they believe any of the controller's instructions are unlawful, and shall notify the controller as soon as possible after becoming aware of a personal data breach of the controller's data.

Data sharing arrangements

4.27 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 GDPR.

4.28 Staff shall consider documenting any systematic, routine disclosure of personal data to another controller in a data sharing agreement that sets out the purposes of the arrangement, the data to be shared, the lawful basis and the operational procedures for sharing data. Guidance on data sharing, including the role of joint controllers, is available on the StaffNet Data Protection pages.

Disclosure of personal data

4.29 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. Guidance on methods of secure data transfer are available on 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.

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

International transfers

4.31 The GDPR allows personal data to be transferred to countries outside the European Economic Area or to international organisations only when one of the conditions specified in the GDPR are met by the controller and the processor. Transfers may be made on the basis of adequacy, an appropriate agreement or in exceptional circumstances. The list of countries deemed 'adequate', links to the model agreements and guidance on the exceptional circumstances available on the StaffNet Data Protection pages.

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

Personal data breaches

4.33 The 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'.

4.34 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 in order to meet the deadline for onward notification of breaches to the regulator and affected data subjects.

4.35 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.

4.36 If required, following the risk assessment, the DPO shall notify a personal data breach to the Information Commissioner. Heads of School / Directors shall ensure that individuals affected by a personal data breach are notified when required.

4.37 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.

4.38 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.

Data subject rights

4.39 The 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 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 with regard to all issues relating to processing of their personal data and the exercise of their rights

4.40 These subject rights are not absolute. The rights are applicable in certain conditions specified in the 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. Guidance on their scope and on common scenarios is available on the StaffNet Data Protection pages. Advice may be sought from the DPO in regard to any particular circumstances.

Data subject rights – requests to the University

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

4.42 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.

4.43 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 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.

4.44 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

4.45 The 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.

4.46 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. Further guidance on the requirements for privacy information is available on the StaffNet Data Protection pages.

4.47 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 in order to meet the GDPR requirement that privacy information is provided at the point personal data is gathered.

4.48 The University may collect and use personal data about data subjects 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 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

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

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

Compliance and monitoring

4.51 The DPO shall maintain Records of Processing Activities for the University's activities as a controller and as a processor. Heads of School / Directors shall ensure sufficient, accurate information is provided to the DPO or the Information Governance team to maintain the Records of Processing Activities.

4.52 The DPO shall monitor and audit 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.

4.53 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 the means by which 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 the means by which 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

This policy shall be reviewed on an annual basis by the DPO and, if required, recommendations for amendment made to the Information Governance Committee.

Glossary of data protection terms

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
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 organization
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 activity
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
GDPR	The General Data Protection Regulation Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016
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. 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
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

Approval/Review History

Version	Date	Action
	University Court 25 May 2004	Approved
	University Court Sep 2010	Updated
	University Court 28 June 2011	Updated
	Data Protection Officer March 2015	Reviewed/minor updates
	Data Protection Officer April 2015	Reviewed/minor updates
3.0	Operating Board 6 Mar 2019	Approved

Policy Metadata

Title	Data Protection Policy
Author / Creator	Iain Gray, Data Protection Officer
Owner	Data Protection Officer
Date published / approved	
Version	V 3.0
Reviewed	January 2019
Date of next review	January 2020
Audience	All staff, partners, suppliers and contractors who work 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