DATA PROTECTION POLICY

1. INTRODUCTION

1.1 Purpose

1.1.1 During the course of the University's activities we will collect, store and process Personal Data about our students, customers, alumni, employees, contractors, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation, reduce risks to both the data subjects and the University, and will provide for successful business operations.

1.1.2 The General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA) replaced the Data Protection Act 1998 on 25 May 2018. In addition, the Privacy and Electronic Communications Regulations (PECR) sit alongside the GDPR and give people specific privacy rights in relation to electronic communications. This Policy specifies how the University governs and manages personal data within a wider Information Governance and Security framework and in accordance with this legislation.

1.1.3 Definitions for all capitalised terms used in this Policy can be found at Annex A.

1.2 Scope

This Policy applies to:

1.2.1 All Personal Data held and Processed by the University. This includes expressions of opinions about individuals and of the intentions of the University in respect of that individual. It includes data held in any system or format, whether electronic or manual;

1.2.2 All members of staff, as well as individuals (including students) conducting work at or for the University and who have access to Personal Data ("you", "your"). This includes temporary, honorary, visiting, casual, voluntary and agency workers, students employed by the University and suppliers, as well as students Processing Personal Data as part of their studies (including research). Note this list is not intended to be exhaustive; and

1.2.3 All locations from which Personal Data is Processed – including off-campus. Each area of the University has responsibility in relation to its own area for (i) ensuring University personnel and students comply with this Policy; and (ii) implementing appropriate practices, processes, controls and training to ensure such compliance.

1.2.4 The governance framework detailed in the Information Governance Framework applies to this Policy.

2. POLICY

2.1 Personal data protection principles

2.1.1 The University adheres to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

(i) processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

(ii) collected only for specified, explicit and legitimate purposes (Purpose Limitation);

(iii) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

(iv) accurate and where necessary kept up to date (Accuracy);

(v) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation); and

(vi) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality) in accordance with the University's Information Security Policy and related guidance.

2.1.2 The University is responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

2.1.3 Full details of the data protection principles and how these should be complied with are contained in the Privacy Guidance.

2.2 Transfer limitation

2.2.1 The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

2.2.2 You may transfer Personal Data outside the EEA only if specific conditions apply. You must comply with the Privacy Guidelines on cross border data transfers.

2.3 Data Subject's rights and requests

2.3.1 Data Subjects have rights with regard to how the University handles their Personal Data. These include rights to:

- **(i)** withdraw Consent to Processing at any time;
- **(ii)** receive certain information about the University's Processing activities;
- **(iii)** request access to their Personal Data that we hold;
- **(iv)** prevent our use of their Personal Data for direct marketing purposes;
- **(v)** ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
- **(vi)** restrict Processing in specific circumstances;
- **(vii)** challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
- **(viii)** request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- **(ix)** object to decisions based solely on Automated Processing, including profiling (ADM);
- **(x)** prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
- **(xi)** be notified of a Personal Data Breach which is likely to result in a high risk to their rights and freedoms;
- **(xii)** make a complaint to the supervisory authority; and
- **(xiii)** in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

2.3.2 You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

2.3.3 You must immediately forward any Data Subject request you receive to dpa@keele.ac.uk and comply with the University's Data Subject response process (see the Privacy Guidance).

2.4 Reporting a Personal Data Breach

2.4.1 The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator (the Information Commissioner in the UK) and, in certain instances, the Data Subject. If a Data Breach is reportable the University must make that report to the ICO and/or the Data Subjects within 72 hours of becoming aware of the breach.

2.4.2 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

2.4.3 If you know or suspect that a Personal Data Breach has occurred, follow the internal notification procedure **without delay**.

2.4.4 Full details on the Breach Reporting procedure can be found in the Privacy Guidance.

2.5 Sharing Personal Data

2.5.1 Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

2.5.2 You may only share the Personal Data we hold with another employee if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

2.5.3 You may only share the Personal Data we hold with third parties, such as our service providers if:

- **(i)** they have a need to know the information for the purposes of providing the contracted services;
- **(ii)** sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- **(iii)** the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- **(iv)** the transfer complies with any applicable cross border transfer restrictions; and
- **(v)** a fully executed written contract that contains GDPR-approved third party clauses has been obtained.

2.5.4 You must comply with the University's guidelines on sharing data with third parties (see the Privacy Guidance).

2.5.5 All other ad-hoc requests for access to Personal Data from third parties (i.e. not from the Data Subject themselves) – including the Police – should be referred to the University's Legal & Information Compliance team at dpa@keele.ac.uk

2.6 Accountability

2.6.1 We will implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The University is responsible for, and must be able to demonstrate, compliance with the data protection principles.

2.6.2 The University must have adequate resources and controls in place to ensure and to document GDPR compliance including:

(i) appointing a suitably qualified Data Protection Officer (DPO) and an executive accountable for data privacy (the SIRO);

(ii) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

(iii) integrating data protection into internal documents including this Policy, Related Policies, Privacy Guidance, Privacy Notices;

(iv) regularly training University personnel on the GDPR, this Policy, Related Policies and Privacy Guidance and data protection matters including, for example, Data Subjects' rights, Consent, legal basis, DPIAs and Personal Data Breaches. The University must maintain a record of training attendance by University personnel; and

(v) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

2.7 Record keeping

2.7.1 The GDPR requires us to keep full and accurate records of all our data Processing activities.

2.7.2 You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents in accordance with the University's record keeping guidance.

2.7.3 These records should include, as a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the retention period for keeping Personal Data and a description of the security measures in place. In order to create such records, asset registers and data maps should be created and maintained.

2.8 Training and audit

2.8.1 We are required to ensure all University personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

2.8.2 You must undergo all mandatory data privacy related training applicable to your areas of activity and ensure your team undergoes similar mandatory training in accordance with the University's mandatory training guidelines.

2.8.3 You must regularly review all the systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

2.9 Privacy By Design and Data Protection Impact Assessments (DPIAs)

2.9.1 We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

2.9.2 We must also conduct DPIAs in respect of high risk Processing.

2.9.3 You should conduct a DPIA (and discuss your findings with the DPO) when implementing any high risk projects involving the Processing of Personal Data including:

- **(i)** use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- **(ii)** Automated Processing including profiling and Automated Decision Making (ADM);
- **(iii)** large scale Processing of Sensitive Data;
- **(iv)** large scale, systematic monitoring of a publicly accessible area; and
- **(v)** any other projects (including research) where there may be significant privacy concerns.

2.9.4 You must comply with the Privacy Guidance on DPIAs and Privacy by Design.

2.10 Marketing

2.10.1 Where we undertake any electronic or telephone direct marketing activities we will ensure that we comply with both the GDPR and the Privacy and Electronic Communications Regulations (PECR).

2.10.2 PECR restrict unsolicited marketing by phone, fax, email, text, or other electronic message. There are different rules for different types of communication. The rules are generally stricter for marketing to individuals than for marketing to companies.

2.10.3 You will often need specific consent to send unsolicited direct marketing. The best way to obtain valid consent is to ask recipients to tick opt-in boxes confirming they are happy to receive marketing calls, texts or emails from you.

2.11 Cookies and similar technologies

2.11.1 Where we employ the use of website cookies or other similar technologies, such as Local Shared Objects, we will comply with both the GDPR and PECR (Regulation 6).

2.11.2 We will ensure that we give clear and comprehensive information about the purposes for which we will use these technologies and we will, where required, seek and record consent to do so.

3. ROLES AND RESPONSIBILITIES

3.1 Council

The University's Council is responsible for approval of the Policy.

3.2 University Executive Group

The University Executive Group is responsible for strategic level implementation of the policy, oversight of compliance with the policy and reporting identified risks to the Council.

3.3 Information Governance Champions

Information Governance Champions hold local responsibility for data protection compliance processed within their teams. A list of IG Champions can be accessed online here.

3.4 Data Protection Officer

The University's Data Protection Officer (DPO) is primarily responsible for advising on and assessing the University's compliance with the DPA and GDPR and making recommendations to improve practice in this area. Further, the DPO acts as the University's primary point of contact for DPA and GDPR-related matters.

3.5 Legal and Information Compliance Team

The Legal and Information Compliance Team are responsible for providing advice, support and guidance in relation to day-to-day data protection matters.

3.6 Staff

3.6.1 As part of their responsibilities (including research) all staff, whether permanent, fixed-term or temporary workers, who Process Personal Data must comply with this Data Protection Policy and the Related Policies and Privacy Guidance.

3.6.2 Staff who supervise students who will be Processing Personal Data as part of their studies (including research) should inform the DPO and the relevant Information Asset Manager(s) before any Processing is commenced.

3.7 Students

3.7.1 Students who are considering Processing Personal Data as part of their studies (including research) must notify and seek approval from their supervisor before any Processing takes place.

3.8 Others working for and on behalf of the University

3.8.1 Others working for and on behalf of the University, third parties such as contractors, consultants and agents, who will handle Personal Data of which the University is the Data Controller, should operate in accordance with the GDPR and details of any such Processing should be subject to a written agreement between the University and the third party in accordance with the Privacy Guidance (Data Sharing). Such third parties include external supervisors, examiners, suppliers or customers.

4. RELATED POLICIES AND PROCEDURES

4.1 This Policy supplements and should be read in conjunction with our other policies and procedures in force from time to time, including without limitation the:

4.1.1 Information Governance Framework;

4.1.2 Information Security Policy;

4.1.3 Records Management Policy and Records Retention Schedule; and

4.1.4 Freedom of Information Policy.

4.2 All procedures and guidelines can be accessed at:

https://www.keele.ac.uk/informationgovernance/fortheuniversity/

5. REVIEW, APPROVAL & PUBLICATION

5.1 Review

5.1.1 The Director of Legal and Information Compliance, Head of Projects and Service Assurance and Senior Information Risk Owner will be responsible for reviewing this Policy on a periodic basisand at least every two years.

5.1.2 This Policy will be reviewed and agreed by the University Executive Committee before final approval.

5.2 Final Approval

This Policy will require final approval from Council.

5.3 Publication

This Policy will be published on the website under the Policy Zone. The University's Information Governance web pages will maintain prominent links to the Policy as appropriate on both external and internal facing pages.

6. ANNEXES

Annex A – Definitions

7. DOCUMENT CONTROL INFORMATION

Document Name	Data Protection Policy
Owner	Clare Stevenson, Director of Legal, Governance & Compliance
Version Number	1.1
Equality Analysis Decision and Date	Not applicable
Approval Date	19 September 2019
Approved By	Council
Date of Commencement	19 September 2019
Date of Last Review	[Day/month/year]
Date for Next Review	September 2022
Related University Policy Documents	Information Governance Framework Information Security Policy Records Management Policy Freedom of Information Policy
Administrative update	10/03/2022; Head of Legal, Governance & Compliance updated to Director of Legal, Governance & Compliance
For Office Use – Keywords	Data protection. privacy, information security, governance, GDPR, General Data Protection Regulation, PECR, DPA18, Data Protection Act 2018.

ANNEX A - DEFINITIONS

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Data Controller: the organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. Keele University is the Data Controller of all Personal Data relating to our employees and Personal Data used in our business for our own public and commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIAs can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR. Reference to the GDPR includes all official guidance on the interpretation of the GDPR by competent bodies including the ICO and Article 29 Working Party.

ICO: Information Commissioner's Office

Information Asset Manager: individuals with operational responsibility for specific information assets and expert knowledge of business processes and how data is used within those processes.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Guidance: the University privacy/GDPR-related guidance provided to assist in interpreting and implementing this Policy and Related Policies, available here: www.keele.ac.uk/informationgovernance

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the University collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee or student privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: the University's policies, operating procedures or processes related to this Policy and designed to protect Personal Data, as detailed at paragraph 4 of this Policy.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

SIRO: Senior Information Risk Owner