DATA PROTECTION POLICY

1. INTRODUCTION

1.1 Purpose

1.1.1 During the course of the University's activities, Personal Data will be collected, stored and processed about students, customers, alumni, employees, contractors, suppliers and other third parties in accordance with the UK GDPR and Data Protection Act 2018. 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 This Policy specifies how the University governs and manages Personal Data within a wider Information Governance framework and in accordance with the legislation and seeks to ensure that Keele University:

- **(i)** is clear about how Personal Data must be processed and the University's expectations for all those who process Personal Data on its behalf;
- **(ii)** complies with the Data Protection Legislation and with good practice;
- **(iii)** ensures the Personal Data entrusted to it is Processed in accordance with Data Subjects' rights;
- **(iv)** protects from risks of Personal Data Breaches and other breaches of Data Protection Legislation.

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

1.2 Scope

1.2.1 This Policy applies to:

- **(i)** All Personal Data held and Processed by the University. This is any data relating to a living and identifiable person, including expressions of opinions about individuals, known as Data Subjects, and of the intentions of the University in respect of those individuals. It includes data held in any system or format, whether electronic or manual and regardless of location;

- **(ii)** All members of staff, as well as individuals (including students) conducting work at or for the University and who have access to Personal Data. 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;

- **(iii)** 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.

1.2.2 The University hosts information for Students' Unions, trade union activities, and information processed by individuals for private ends, including in staff, student and alumni email accounts. Where the University does not determine the means and purpose of Personal Data Processing, and it is not acting on behalf of another Data Controller, it is neither Data Controller nor a Data Processor of the information being processed, regardless of whether the processing takes place on University systems or platforms.

1.2.3 This Policy forms part of, and should be read in conjunction with, the University's Information Governance Framework.

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 UK GDPR. The University is responsible for, and must be able to demonstrate compliance with, the data protection principles listed below, which state that Personal Data must 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 In addition, the UK GDPR requires the University to be accountable for and demonstrate compliance with the above six principles.

2.2 Accountability and Record Keeping

2.2.1 The University must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with the data protection principles. Failure to do so could result in breach of legislation, reputational damage, or financial implications due to fines.

2.2.2 The University must have adequate resources and controls in place to ensure and to document UK 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 Data Protection Impact Assessments (DPIAs) where Processing presents a high risk to the rights and freedoms of Data Subjects;
(iii) integrating data protection into University documents including policies and procedures, privacy guidance and Privacy Notices and maintaining a Record of Processing Activities (ROPA) and a record of Personal Data Breaches;

(iv) training University staff on compliance with Data Protection Legislation and keeping a record accordingly;
(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;
(vi) maintaining accurate corporate records reflecting the University's Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

2.3 Data Subject's rights and requests

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

a. where the legal basis of the Processing is 'Consent', to withdraw that consent at any time;
b. ask for access to the Personal Data that the University holds (Subject Access Request);
c. object at any time to the University's use of the Personal Data for direct marketing purposes;
d. object to the University's processing of Personal Data in limited circumstances where the University is processing the data on the lawful basis of 'Public Task' or 'Legitimate Interests';
e. ask the University to erase Personal Data:
    i. if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
    ii. if the only lawful basis of processing is consent and that consent has been withdrawn and there is no other lawful basis on which the University can Process that Personal Data;
    iii. if the Data Subject successfully objects to the Processing where the lawful basis is "Legitimate Interests" or "Public Task" and the University has no overriding reason to retain the data;
    iv. if the Data Subject has objected to the Processing for direct marketing purposes;
    v. if the Processing is unlawful.

f. ask the University to rectify inaccurate data or to complete incomplete data;
g. restrict processing in specific circumstances;
h. request a copy of the safeguards under which Personal Data is transferred outside of the UK to any "Third Country";
i. not be subject to decisions based solely on Automated Processing, including profiling, except where:
    i. necessary for entering into, or performing, a contract with the University;
    ii. it is based on the Data Subject's Explicit Consent and is subject to safeguards; or
    iii. is authorised by law and is also subject to safeguards;

j. be notified of a Personal Data breach where such breach is likely to result in a high risk to Data Subjects' rights and freedoms;
k. make a complaint to the ICO; and
l. in limited circumstances, receive or ask for Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

2.3.2 The University must verify the identity of an individual requesting data under any of the rights listed above.

2.3.3 Requests must be complied with within one month of receipt or, in limited circumstances within a total of three months. Staff must immediately forward any Data Subject Rights Requests received to the Legal and Information Compliance team at dpa@keele.ac.uk.

2.4 Reporting a Personal Data Breach

2.4.1 A data breach is an event or action resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data held and processed by the University.

2.4.2 The UK 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 to the ICO, the University must make that report within 72 hours of becoming aware of the breach.

2.4.3 Where the University is not the Data Controller and becomes aware of any Personal Data Breach relating to data that it holds and / or processes on behalf of another organisation, it is obligated to inform that organisation as soon as it becomes aware of the same.

2.4.4 In some cases, it may be determined that the affected Data Subjects should be notified of a Personal Data Breach, which will be determined by the Legal and Information Compliance team as part of the internal Data Breach handling procedure.

2.4.5 All staff have a duty to notify the University's Data Protection Officer (DPO) of any confirmed or suspected Personal Data Breach. If staff know or suspect that a Personal Data Breach has occurred, they should **immediately** report the incident by following the instructions available online at https://keeleacuk.sharepoint.com/sites/lgc-intranet/SitePages/Data-breach-reporting.aspx. Staff must retain all evidence relating to Personal Data Breaches to enable the University to maintain a record of such breaches, as required by the UK GDPR.

2.5 Sharing Personal Data

2.5.1 Personal data should only be shared with third parties where there is a lawful basis to do so and any Processing must be in accordance with data protection principles. Sharing will usually have been communicated to Data Subjects in a Privacy Notice beforehand.

2.5.2 Where a third party is Processing the Personal Data on the University's behalf, staff must undertake appropriate due diligence on the third party and enter into a Data Sharing Agreement with the Processor that complies with the UK GDPR's requirements for such agreements. Where the University is a Joint Controller, a Data Sharing Agreement must be entered into; such an agreement should also be considered where the University is sharing Personal Data with another independent Data Controller.

2.5.3 The transfer of any personal data to an unauthorised third party would constitute a breach of the UK GDPR principles and may constitute a Personal Data Breach. Ad-hoc requests for access to Personal Data from third parties (i.e. not from the Data Subject themselves), such as the Police, General Medical Council, MPs etc., should be referred to the University's Legal and Information Compliance team via dpa@keele.ac.uk

2.6 International Data Transfers

2.6.1 The UK GDPR restricts data transfers to countries outside the UK or European Economic Area (EEA) in order to ensure that the level of data protection afforded to Data Subjects is not undermined.

2.6.2 Personal Data may only be transferred outside the UK or EEA if one of the following conditions applies:

(i) the country is covered by UK 'adequacy regulations';
(ii) appropriate safeguards are in place such as binding corporate rules, the UK's International Data Transfer Agreement (IDTA) and/or the EU's standard contractual clauses with UK addendum, an ICO approved code of conduct or a certification mechanism;
(iii) the Data Subject has provided explicit Consent to the proposed transfer after being informed of any potential risks; or
(iv) the transfer is necessary for one of the other reasons set out at Article 49 of the UK GDPR

2.6.3 When Personal Data is being considered for transfer, a Transfer Risk Assessment must be completed and staff should seek guidance from the Legal and Information Compliance team via dpo@keele.ac.uk.

2.7 Training and process review

2.7.1 The University is required to ensure that all employees undergo adequate training to enable them to comply with Data Protection Legislation. The University has in place a mandatory training module which must be undertaken by all staff upon induction and annually thereafter, as required.

2.7.2 Information Asset Owners (IAO) must ensure that the systems and processes under their control are reviewed regularly to confirm that they are adequate and effective for the purposes of facilitating compliance with the University's obligations under this policy and that sufficient resources are in place to ensure proper use and protection of Personal Data.

2.7.3 The University shall make available resources, tools, advice and information (including links to relevant external advice and guidance such as that published by the Information Commissioner's Office) relating to Data Protection to enable staff to comply with the Data Protection Legislation. Further information is available on the ICO website: https://ico.org.uk/

2.8 Data Protection Impact Assessments (DPIAs)

2.8.1 A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks involved in projects, processes and activities involving the processing of personal data. A DPIA must be completed when such processing is likely to result in a high risk to the Data Subjects and their Personal Data.

2.8.2 A DPIA should be completed at the earliest design stages of a project and must:

(i) describe the nature, scope, context and purposes of the processing;
(ii) assess necessity, proportionality and compliance measures;
(iii) identify and assess risks to individuals; and
(iv) identify any additional measures to mitigate those risks.

2.8.3 A DPIA must be carried out in consultation with the Legal and Information Compliance team and other relevant individuals and/or stakeholders, as appropriate. To identify when a DPIA

is required the University's DPIA Screening Questions should be completed as a first step via the intranet. Where a DPIA is not found to be a requirement, one may be advised to be completed as part of best practice.

2.8.4 Completed DPIAs must be kept under review throughout the lifecycle of a project and may be disclosed to the public as part of Freedom of Information legislation.

2.9 Cookies and similar technologies

2.9.1 Where the University employs the use of website cookies or other similar technologies, it will comply with both the UK GDPR and Privacy and Electronic Communications Regulations (PECR) (Regulation 6).

2.9.2 The University will ensure that it gives clear and comprehensive information about the purposes for which these technologies are used and will, where required, seek and record consent to do so.

3 ROLES AND RESPONSIBILITIES

3.1 Council

The University's Council is responsible for overseeing the governance of the University and for safeguarding its assets (including Information Assets) and for approval and oversight of the implementation of this policy.

3.2 Information Asset Owners (IAOs)

The IAOs are responsible for strategic level implementation of this policy, including staff compliance with the same which encompasses mandatory training, adherence to appropriate processes and ensuring that resources are available within their areas to enable the completion and review of the University Record of Processing Activities (ROPA).

3.3 Data Protection Officer (DPO)

The University's DPO is an independent role and is responsible for advising on and assessing the University's compliance with Data Protection Legislation and making recommendations to improve practice in this area. Further, the DPO acts as the University's primary point of contact for Data Protection Legislation related matters.

3.4 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.

3.5 Staff

3.5.1 As part of their responsibilities 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 Procedures.

3.5.2 All staff are responsible for:

(i) adhering to the data protection principles as set out at section 2.1 when Processing Personal Data on behalf of the University;

(ii) completing mandatory data protection/information security training upon induction, and thereafter training as required;

(iii) following University data protection advice and guidance relevant to their role, irrespective of whether access and/or processing of Personal Data is through

University-owned and managed systems, or through personal or third party's systems and devices;

(iv) only Processing Personal Data as is necessary for fulfilling their role as set out by the University in its Privacy Notices, and not disclosing it unnecessarily or inappropriately;

(v) recognising and reporting data breaches internally via the appropriate procedures, and cooperating with any remedial work;

(vi) cooperating with the University's fulfilment of data subject rights requests (including Data Subject Access Requests);

(vii) advising students who are using Personal Data in their studies and research of relevant advice, guidance and tools/methods to enable them to handle such Personal Data in accordance with this Policy and other related policies and procedures;

(viii) implementing data protection by design and default principles, as appropriate, from the start and throughout the lifecycle of any project they are responsible for including, but not limited to, completing Data Protection Impact Assessments where required, updating Records of Processing Activity and ensuring that Privacy Notices are appropriately updated.

3.6 Students

3.6.1 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 and follow all appropriate University policy and procedures.

3.6.2 If a student is employed by the University, they will have the responsibilities of all staff as set out above in respect of any Processing of Personal Data carried out in the course of their employment.

3.7 Contractors, Short Term and Voluntary Staff

3.7.1 The University is responsible for the Processing of Personal Data by anyone working on its behalf. Line managers who employ third-parties, such as contractors, short term or voluntary staff, must ensure that they are appropriately screened for the data they will be Processing.

3.7.2 All third-parties must abide by this Policy.

4 RELATED POLICIES AND PROCEDURES

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

4.1.1 Information Governance Framework;

4.1.2 Data Breach Management Procedure;

4.1.3 Information Security Policy;

4.1.4 Data Classification and Handling Policy;

4.1.5 Records Management Policy and Records Retention Schedule;

4.1.6 Freedom of Information Policy;

4.1.7 Appropriate Policy.

4.2 All procedures and guidelines can be accessed at: www.keele.ac.uk/informationgovernance/fortheuniversity/

5 REVIEW, APPROVAL & PUBLICATION

5.1 Review
The Policy will be reviewed and agreed by the University Executive Committee and Audit & Risk Committee before being recommended for final approval.

5.2 Final Approval
This Policy will require final approval from Council.

5.3 Publication
This Policy will be published on the University's website within the Policy Zone. The University's Legal and Information Compliance 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	2.0
Equality Analysis Decision and Date	Not applicable
Approval Date	23 November 2023
Approved By	Council
Date of Commencement	19 September 2019
Date of Last Review	18 October 2023
Date for Next Review	23 November 2026
Related University Policy Documents	Information Governance Framework; Data Breach Management Procedure; Information Security Policy; Data Classification and Handling Policy; Records Management Policy and Records Retention Schedule; Freedom of Information Policy; Appropriate 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, information governance, EU GDPR, UK GDPR, General Data Protection Regulation, PECR, DPA18, Data Protection Act 2018.

ANNEX A

Term	Definition
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, behaviour, location or movements. Profiling is an example of **Automated Processing**.
Consent	A freely given, specific, informed and unambiguous indication of a **Data Subject**'s wishes by which they, by a statement or by a clear affirmative action, signify agreement to the **Processing** of **Personal Data** relating to themselves.
Data Controller	The individual, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the **Processing** of **Personal Data**
Data Processor	**Data Processors** act on behalf of, and only on the instructions of, the relevant **Data Controller** for the purposes of **Processing** that **Data Controller's Personal Data**.
Data Protection Act 2018 (DPA)	Regulates the **Processing** of information relating to individuals, including the holding, obtaining, recording, use or disclosure of such information. The UK's Data Protection Act 2018, which supports and should be read in conjunction with the UK General Data Protection Regulation (**UK GDPR**).
Data Protection Impact Assessment (DPIA)	A process designed to help organisations identify and mitigate privacy risks associated with proposed data processing activities. It is a legal requirement to conduct a **DPIA** for **Processing** that is likely to result in a high risk to individuals.
Data Protection Legislation	The UK General Data Protection Regulation (**UK GDPR**) and UK Data Protection Act 2018 (**DPA**).
Data Protection Officer (DPO)	The **DPO** assists the University to operate in compliance with **Data Protection Legislation** by improving accountability, providing advice and helping to monitor compliance. They also help implement the requirements of **Data Protection Legislation** across the organisation such as: i. The principles of data processing ii. Data Subjects' rights and complaints iii. Data protection by design and by default iv. Records of processing activities v. Security of processing vi. Notification and communication of data breaches
Data Sharing Agreement (DSA)	A legal contract outlining the information that parties agree to share and the terms under which the sharing will take place.
Data Subject	An identifiable living individual whose **Personal Data** is processed by a **Data Controller** or **Data Processor**

EEA	The 27 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).
Freedom of Information Act 2000 (FOIA)	The Freedom of Information Act 2000 **(FOIA)** provides members of the public in the UK and globally the right to request information from public authorities
Freedom of Information request (FOI)	A request made to the University for information under the Freedom of Information Act 2000 (**FOIA**)
Individual Rights Requests (IRR)	All living individuals (**Data Subjects**) have rights in relation to the **Processing** of their **Personal Data** being held or processed by an organisation: • The right to be Informed - e.g. fair processing/privacy notices and information • The right of Access - e.g. subject access requests (**SARs**) • The right to Rectification - e.g. correcting data • The right to Erasure – e.g. deleting or removing data • The right to Restrict Processing – e.g. stopping data being used • The right to Data Portability – e.g. transferring data easily • The right to Object – e.g. challenging what the Data Controller is doing with data • Rights in Relation to Automated Decision Making and Profiling – e.g. ensuring safeguards are in place so potentially damaging decisions about an individual without any human involvement.
Information Asset	Information or data; the systems and locations in which it is stored; and the means by which it is accessed.
Information Asset Owner (IAOs)	Senior member of staff of Directorate / Faculty who has overall responsibility for specific **Information Assets** and who ensures that those assets are handled and managed appropriately, protected against risk and their value to the organisation is recognised.
Information Asset Register	An **Information Asset Register** documents the types of information held by an organisation with the purpose of helping it to understand and manage its **Information Assets** (e.g. identify duplication, increase business efficiency and manage risks).
Information Commissioner's Office (ICO)	The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Information Governance	Comprises **Information Management** and **Information Security**: set of multi-disciplinary structures, policies, procedures, processes and controls required to manage information in support of an organisation's regulatory, environmental, operational and risk requirements. It allows organisations to ensure information is processed lawfully, securely, efficiently and effectively.

Information Management	The collection, storage, classification, handling, dissemination, archiving and destruction of information / data, whether in electronic or physical form, throughout its lifecycle and in compliance with business and regulatory requirements.
Information Security	The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction, including from cyber-attacks, to ensure confidentiality, integrity and availability.
Lawful Basis	At least one of six lawful bases must apply whenever an organisation processes **Personal Data**: • Consent: the individual has given clear consent to process their **Personal Data** for a specific purpose. • Contract: the **Processing** is necessary for a contract, or to take specific steps before entering into a contract. • Legal obligation: the **Processing** is necessary to comply with the law (not including contractual obligations). • Vital interests: the **Processing** is necessary to protect someone's life. • Public task: the **Processing** is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law. • Legitimate interests: the **Processing** is necessary for the organisation's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's **Personal Data** which overrides those legitimate interests. (This cannot apply for are a public authority, such as a University, **Processing** data to perform its official tasks - Public Task must be used instead)
Personal Data	Any information relating to an identifiable living individual (**Data Subject**); i.e. can be identified directly or indirectly, for example by an identifier such as name, identification number, location data, an online identifier and/or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.
Personal Data Breach	A **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, **Personal Data**. This includes breaches that are the result of both accidental and deliberate causes.
Privacy and Electronics Communications Regulations 2019 (PECR)	Regulations which give people specific privacy rights in relation to electronic communications including specific rules on: • marketing calls, emails, texts and faxes; • cookies (and similar technologies); • keeping communications services secure; and • customer privacy as regards traffic and location data, itemised billing and directory listings.
Privacy by Design	Appropriate technical and organisation measures which are implemented in an effective manner to ensure compliance with the **UK GDPR**.
Privacy Notice	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 (e.g. employee or student privacy notices) or they may be stand alone, one-time privacy statements covering **Processing** 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, retrieving, using, erasing or destroying it. **Processing** also includes transmitting or transferring **Personal Data** to third parties.
Record of Processing Activities (ROPA)	The Record of Processing Activities **(ROPA)** is an inventory of the **Processing** of **Personal Data** and an overview of what is happening with the concerned **Personal Data**. The recording obligation is included at article 30 of the UK GDPR.
Special Category Data	Specific type of **Personal Data** revealing: • racial or ethnic origin; • political opinions; • religious or philosophical beliefs; • trade union membership; • the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person; • health data; • data concerning a person's sex life or sexual orientation
Subject Access Request (SAR)	A request made for an individual's own **Personal Data**, or someone acting on their behalf with their permission, under the **UK GDPR** Article 15
Third Party Request (TPR)	A request for an individual's **Personal Data** made by a third party, such as the Police, an MP etc.
UK GDPR	**UK GDPR** means the European Union General Data Protection regulation (EU GDPR) as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018 and sits alongside an amended version of the Data Protection Act 2018 (**DPA**). The **UK GDPR** is a legal framework that sets out principles for the collection and processing of personal information.