Data Protection Policy

Document Title: Data Protection Policy			
Version No.	2.1	Policy Owner	LGS
Superseded version	2.0	Author Role Title	Head of Information Governance L&GS
Approval Date	18.05.2021	Approved by	UET
Effective Date	09.07.2019	Review Date	June 2022

Data Protection Policy

1. Introduction

In order to carry out its functions, to provide its services and to meet its legal and regulatory obligations, the University gathers and processes Personal Data about its students, staff and other individuals.

The University is committed to protecting the privacy of all individuals by ensuring the fair, responsible and transparent use of all Personal Data that it holds in full compliance with the safeguards and requirements of the General Data Protection Regulations and the Data Protection Act 2018 (together "Data Protection Law"). The University aims to comply with legislation to the fullest extent possible, and has a low risk appetite and tolerance towards data protection risk management (in accordance with the University's Risk Management and Framework Policy).

This Policy and the accompanying Data Protection Code of Practice set out minimum standards that the University must comply with in order to satisfy this commitment and seeks to ensure that all Policy users are clear about how Personal Data must be processed in order to comply with Data Protection Law and best practice.

2. Scope

This Policy applies to all University staff and students, and any other individual processing Personal Data held by or on behalf of the University.

This Policy applies to all recorded information which relates to identified or identifiable individuals, irrespective of the format in which that information is held and regardless of the location where Personal Data is stored e.g. it applies equally to Personal Data stored on an employee or student's own device.

This Policy does not apply to information processed by the Students' Union, by trade unions, or by any other entities which are located in University premises but are not owned or managed by the University and which have separate legal identities.

3. Guidance and related policies

This Policy is accompanied by the Data Protection Code of Practice which is to be followed by all those to whom this policy applies in order to achieve the University's policy objectives. Reference should also be had to the University's Information Security Policy and the Data Breach Management Policy. Copies of the Data Protection Code of Practice and related policies are available from the Information Governance unit in Legal & Governance Services (email: dpo@tees.ac.uk) and are also accessible from the Legal & Governance Services intranet available here.

4. Definitions

All definitions in this policy have the same meaning as under Data Protection Law. For ease of reference a number of definitions are set out below:

Personal Data	means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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 natural person.
Special categories of Personal Data	known previously as sensitive Personal Data, special categories of Personal Data are those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Processing	means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, 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.
Controller	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

5. Chain of Accountability

The University as Data Controller has a corporate responsibility to process Personal Data with due regard to the rights and freedoms of individuals, and to comply with the requirements of Data Protection Law.

All public bodies are required to appoint a Data Protection Officer (DPO). It is the role of the DPO to assist the University in monitoring internal compliance, inform and advise on data protection obligations and act as a contact point for data subjects

and the Information Commissioner's Office (ICO). The DPO also helps demonstrate compliance in accordance with the enhanced focus on accountability.

The Information Governance Team has responsibility for providing advice on information governance issues, including data protection for processing and recording requests for access to Personal Data and other rights existing under Data Protection Law, for managing relevant complaints, for raising internal and external awareness of the University's obligations, which includes training, and for notifying the Information Commissioner of the details of the Data Protection Officer along with payment of the annual fee.

USMT members must ensure that the activities and processes within their school or departments (as applicable) are compliant with this Policy and related Data Protection Code of Practice, and that their staff have a sufficient awareness and knowledge of relevant requirements and that appropriate processes are in place to ensure compliance.

Local Information Governance Champions will be assigned within each School and Department by the Dean/Director as a champion for ensuring a consistent approach to implementing this Policy and Code of Practice and to liaise as appropriate with Legal & Governance Services in ensuring and demonstrating compliance.

6. Data Protection Principles

Any individual processing Personal Data should adhere to the following Data Protection principles which are set out in Article 6 of the GDPR:

(a) Personal Data shall be processed lawfully, fairly and in a transparent manner;
(b) Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
(c) Personal Data shall be adequate, relevant and limited to what is necessary in relation to the processing purpose;
(d) Personal Data shall be accurate and, where necessary, kept up to date;
(e) Personal Data shall be kept in a form which permits identification of subject for no longer than is necessary for the processing purpose;
(f) Personal Data shall be processed securely and in a manner that protects against unauthorised or unlawful processing, loss, destruction or damage

The University as Data Controller shall be responsible for demonstrating compliance with the above principles and will implement appropriate technical and organisational measures to ensure compliance.

The Data Protection Code of Practice details how these Principles are to be applied in practice to University activities.

7. Lawful grounds for processing

The first data protection principle stipulates that Personal Data shall be processed lawfully. Processing can only be carried out where there is a lawful basis. Article 6 of the GDPR sets out the lawful grounds for processing Personal Data. Article 9 sets out the lawful grounds for processing Special Category Data. These lawful grounds are set out below:

Article 6 lawful grounds

6(1)(a)	Consent of the data subject
6(1)(b)	Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract with the data subject.
6(1)(c)	Processing is necessary to comply with a legal obligation.
6(1)(d)	Processing is necessary to protect the vital interests of a data subject or another person.
6(1)(e)	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 Data Controller.
6(1)(f)	Processing is necessary for the purposes of legitimate interests pursued by the Data Controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Article 9 lawful grounds

9(1)(a)	Explicit consent of the data subject unless reliance on consent is prohibited by EU or UK law.
9(1)(b)	Processing is necessary to carry out obligations under employment, social security or social protection law, or a collective agreement.
9(1)(c)	Processing is necessary to protect the vital interests of a data subject or other individual where the data subject is physically or legally incapable or giving consent.
9(1)(d)	Processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing only relates to members or former members and there is no disclosure to a third party without consent.
9(1)(e)	Processing relates to Personal Data manifestly made public by the data subject.
9(1)(f)	Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
9(1)(g)	Processing is necessary for the purpose of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social-care or treatment or management of health or social care systems and services on the basis of EU or UK law or a contract with a health professional.
9(1)(h)	Processing is necessary for reasons of public interest in the area of public health.
9(1)(i)	Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes with appropriate safeguards applied.

An individual should confirm and document which lawful ground applies to its processing activity prior to any processing activity being carried out.

8. Rights of Individuals

The University will comply with the rights given to individuals under Data Protection Law, which are as follows:

(a) The right to be informed;

(b) The right to access - This is often referred to as a subject access request or SAR. The University is required to supply a copy of relevant information, subject to any exemptions, within one calendar month of receipt of a valid request. The University may require evidence of the identity of the requestor. Information will be provided free of charge unless further copies are required or the request is considered manifestly unfounded or excessive.

(c) The right to request Personal Data is rectified, if inaccurate;

(d) The right to request erasure of their Personal Data (in certain circumstances);

(e) The right to request that the processing of their Personal Data is restricted;

(f) The right of portability in relation to their Personal Data;

(g) The right to object to the processing of their Personal Data;

(h) The right to object to processing which involves automated decision making or profiling.

These are not unqualified rights and each request will be considered on its merits. Reference should be had to the University's Privacy Notices.

Members of staff who receive a request to exercise any of the above rights must contact the Information Governance Team without delay so that the request can be processed within the prescribed time for a response.

Individuals who wish to exercise any of the above rights should contact the University's Data Protection Officer via Legal & Governance Services: dpo@tees.ac.uk or 01642 342093 / 01642 342563.

9. Privacy By Design and Default and Data Protection Impact Assessments

The University is required to ensure that it follows a procedure of Privacy by Design when processing personal data. This requires the University having the necessary technical and organisational measures to ensure that by default, only personal data which is necessary for any particular purpose is processed. The University must also carry out Data Privacy Impact Assessments (DPIAs) in respect of high risk processing. It is mandatory to carry out a DPIA in the following circumstances:

- When using new technologies
- When using automated processing or profiling
- Large scale processing, in particular of special category data
- Large scale systematic monitoring of a publicly accessible area

The University is also required to provide privacy information to Data Subjects in the form of privacy notices. These should provide clear, easy to understand information about what the University does with Data Subjects' Personal Data. Reference should be had to the Data Protection Code of Practice for what information needs to be contained in privacy notices.

10. Responsibilities of Staff

All staff must comply with the requirements of this Policy and the Data Protection Code of Practice.

Staff may only process Personal Data to the extent to which they have been specifically authorised by the University, or are generally authorised as part of their role within the University.

Staff are responsible for ensuring any Personal Data processed in the course of their employment is managed securely. Specifically, individuals are responsible for ensuring that Personal Data in their possession is not left unsecure, for example in meeting rooms, public spaces, open plan environments or mobile devices, without adequate protection.

Staff must ensure that existing and new business processes, activities and systems (e.g. IT software) are compliant with the requirements of Data Protection Law and this Policy and Data Protection Code of Practice, and that their local Data Protection Coordinator is made aware of any significant changes to the processing of Personal Data. Specific advice can be provided by Information Governance Team as required.

Staff must undertake DPIAs, with support from Information Governance Team, in the circumstances referred to above prior to commencing any high risk processing activity in accordance with the Data Protection Code of Practice and University guidance on DPIAs.

Staff must ensure that privacy information is communicated to Data Subjects at the point of collection of Personal Data.

Academic staff are responsible for ensuring that their students are fully informed about their responsibilities under the Act with regard to any specific coursework or research which involves the gathering or processing of Personal Data. Academic staff authorising the processing of Personal Data by students for the purpose of coursework or research are responsible for the monitoring of that processing.

Research Ethics Committees both at school and University level will take appropriate measures to ensure that the research activities of students and staff are compliant with data protection requirements.

In relation to any processing which is not undertaken in the course of University activities, i.e. where the University is not the Data Controller, individuals are responsible for their own compliance with Data Protection Law

11. Responsibilities of Students

In connection with their academic studies/research, all University students have the following responsibilities:

- to notify an appropriate member of staff, usually their tutor, if they intend to process information about identifiable individuals as part of their academic studies/research;

- to only process Personal Data for use in academic studies/research which has been expressly authorised by a member of staff or the appropriate Research Ethics Committee;

- to comply with any regulations or requirements implemented by the University or by a member of University staff in order to facilitate compliance with Data Protection Law; and

- to have reference and to adhere to the University Policy, Procedures and Guidelines for Research Ethics.

In relation to any activities not specifically authorised by the University, students processing Personal Data are responsible for their own compliance with Data Protection Law.

12. Reporting a Personal Data Breach

It is a requirement of the GDPR that any personal data breaches are reported to the ICO where there is a serious risk to the rights and freedoms of a Data Subject. The University has a Data Breach Management Policy which is to be followed in the event of a breach. All breaches should be reported in accordance with that policy to dpo@tees.ac.uk

13. Transfer outside the EU/EEA

The UK has incorporated the GDPR into the withdrawal bill and pending an adequacy decision, the EU-UK Trade and Cooperation Agreement contains a bridging mechanism that allows the continued free flow of personal data from the EU/EEA to the UK until adequacy decisions come into effect, for up to six months. The GDPR requires Data Controllers to ensure that any Personal Data sent to any country outside the EU/EAA is afforded the same level of protection as in the EU.

Transfers outside the EU/EAA are only permitted in the following situations:

- The European Commission has issued a decision confirming the country receiving the Personal Data is provides an adequate level of protection;

- Appropriate safeguards are in place such as binding corporate rules or standard contractual clauses;

- The data subject has provided explicit consent to the proposed transfer having been informed of all the risks;

- The transfer is necessary for one of the reasons set out in the GDPR including:

    - The performance of a contract;

- Reasons of public interest;
- For the establishment or defence of legal claims;
- In the Vital Interests of a Data Subject.

Where transfers are being made out of the EU/EEA, advice should be sought from the Information Governance Team to ensure compliance.

14. Training and Audit

The University will ensure that all staff receive appropriate training to enable them to comply with this Policy and Data Protection Law. Data Protection training is mandatory. Any individual who does not think they are sufficiently aware of Data Protection Law should contact Legal & Governance Services to arrange additional training. The University will regularly test our systems and processes to monitor compliance.

15. Policy Enforcement

Failure to follow this Policy and the Data Protection Code of Practice may result in disciplinary action.