Data Protection Policy

Document Title: Data Protection Policy			
Version No.	1.2	Policy Owner	LGS
Superseded version	1.1	Author Role Title	Deputy Director L&GS
Approval Date	25/05/2018	Approved by	EPC
Effective Date	25/05/2018	Review Date	25/05/2019

Table of Contents

Data Protection Policy 2
Appendix 1 – Subject Access Requests 8
Appendix 2 – Code of Practice 12
Appendix 3 – Confidential Waste Disposal Procedure 19

Data Protection Policy

Introduction

In order to carry out its functions, to provide its services and to meet its obligations, the University gathers and processes personal data about its students, staff and other individuals. The University is committed to protecting the privacy of individuals by ensuring the fair, responsible and transparent use of all personal data that it holds, including compliance with the safeguards and requirements of the General Data Protection Regulations and the Data Protection Act 2018. This Policy and its associated Code of Practice and Procedure set out the minimum standards with which all sections of the University must comply in order to satisfy this commitment.

1. Scope

1.1 This Policy applies to all University staff and students, and any other individual authorised to access University information.

1.2 This Policy applies to all recorded information which relates to identified or identifiable individuals, irrespective of the format in which that information is held.

1.3 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.

2. Objectives

This Policy and its accompanying Procedure and Code of Practice aim to ensure that:

2.1 Personal data gathered and processed by the University is done so fairly, responsibly and transparently, and with full consideration for the confidentiality and privacy of each individual.

2.2 The University complies with all requirements of the Data Protection Act 2018, and all subsidiary or related legislation.

3. Guidance

This Policy is accompanied by a Code of Practice which details the practical implications of the above objectives to University activities including incident management procedures;

3.1 Guidance to support the objectives of this Policy is available from Legal & Governance Services) (email: dpo@tees.ac.uk; tel: x.2060) and is also accessible from the Legal & Governance Services intranet available here.

4. Definitions

The following definitions should be applied to the interpretation of this Policy and its accompanying Procedure and Code of Practice:

Personal data	Any information relating to an identifiable living individual, including expressions of opinion or intentions. This now also explicitly extends to IP addresses.
Special categories of personal data	Known previously as sensitive personal data, means any information about an individual's ethnicity, political opinions, religious beliefs, or other beliefs of a similar nature, membership of a trade union, disability, sexual orientation, the commission or alleged commission by them of any criminal offence, or any proceedings for any offence committed or alleged to have been committed by them.
Processing	Any operation which is performed on personal data whether or not by automated means such as collection, use, disclosure, storage and deletion.

5. Responsibilities

The University 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 the Data Protection Act 2018. Overall responsibility for this Policy lies with the University Secretary.

Legal & Governance Services has responsibility for providing advice on information compliance issues, for processing and recording requests made under section 7 of the Data Protection Act, for managing relevant complaints, for raising internal and

external awareness of the University's obligations, and for maintaining the University's Registration with the Information Commissioner.

Deans and Directors of each School and Department must ensure that the activities and processes within their departments are compliant with this Policy and Code of Practice, and that their staff have a sufficient awareness and knowledge of relevant requirements.

Local Data Protection Coordinators will be assigned within each School and Department by the Dean/Director, with the functions of: providing a local point of contact for DPA issues, and reporting significant changes in the processing of personal data to Legal & Governance Services.

5.1. Responsibilities of Staff

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

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

5.1.3. Staff are responsible for ensuring personal data they possess in undertaking their role, is managed securely. Specifically, individual are responsible for ensuring that personal data in their possession is not left unsecure in meeting rooms, public spaces or on desks within open plan environments.

5.1.4. Staff must ensure that existing and new business processes, activities and systems (e.g. IT software) are compliant with the requirements of the Data Protection Act and this Policy and 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 Legal & Governance Services as required.

5.1.5. 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.

5.1.6. Research Ethics Committees will take appropriate measures to ensure that the research activities of students and staff are compliant with Data Protection requirements.

5.1.7. 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

the Data Protection Act, including Notification with the Information Commissioner if appropriate.

5.1.8. The University's Staff Disciplinary Procedure may be used, if appropriate, should there be a breach of this Policy.

5.2. Responsibilities of Students

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

1. 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;
2. 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;
3. to comply with any regulations or requirements implemented by the University or by a member of University staff in order to facilitate compliance with the Data Protection Act.

5.2.2. In relation to any activities not specifically authorised by the University, students processing personal data are responsible for their own compliance with the Data Protection Act, including Notification with the Information Commissioner if appropriate.

5.2.3. The University's Student Disciplinary Procedure may be used, if appropriate, should there be a breach of this Policy.

6. Data Protection Principles

6.1. The University will comply with the seven Data Protection principles as required by the Data Protection Act, which provide that:

1. Personal data shall be processed lawfully, fairly and in a transparent manner;
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Personal data shall be adequate, relevant and limited to what is necessary in relate to the processing purpose;
4. Personal data shall be accurate and, where necessary, kept up to date;
5. Personal data shall be kept in a form which permits identification of subject for no longer than is necessary for the processing purpose;
6. Personal data shall be processed securely and in a manner that protects against unauthorised or unlawful processing, loss, destruction or damage
7. The Data Controller shall be responsible for demonstrating compliance with the above principles.

6.2. The accompanying Code of Practice informs the practical application of these Principles to University activities.

7. Rights of Individuals

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

1. The right to be informed what personal data the University processes about them and to request a copy;
2. The right to request personal data is rectified if inaccurate;
3. The right to request erasure of their personal data (in certain circumstances);
4. The right to request that the processing of their personal data is restricted;
5. The right of portability in relation to their personal data;
6. The right to object to the processing of their personal data;

7. The right to object to processing which involved automated decision making or profiling.

7.2. Individuals who wish to exercise the above rights should contact the University's Data Protection Officer via Legal & Governance Services: dpo@tees.ac.uk. Any such requests directed to other members of staff should be forwarded to the DPO as soon as possible.