Data Protection Code of Practice

Document Title: Data Protection Code of Practice			
Version No.	2.0	Policy Owner	LGS
Superseded version	1.1	Author Role Title	Head of Information Governance L&GS
Approval Date	09.07.19	Approved by	UET
Effective Date	09.07.19	Review Date	July 2020

Data Protection Code of Practice

Contents

---

1. Introduction

This Code of Practice accompanies the University's Data Protection Policy and provides practical guidance around how to implement and adhere to the Data Protection Policy. Definitions in this Code of Practice are the same as in the Data Protection Policy and reflect definitions in the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (together referred to as Data Protection Law).

2. General requirements when processing Personal Data

This section applies to any processing of Personal Data, including collection, use, storage, disclosure and disposal.

Personal Data must be processed in line with the Data Protection principles of the GDPR. This section describes what this means in practical terms.

(a) Personal Data shall be processed lawfully, fairly and in a transparent manner.

This means that staff will:

- identify an appropriate lawful basis (refer to the Data Protection Policy for a list of lawful bases) for any processing;
- provide privacy notices that clearly define the nature and purpose of processing and state the lawful basis for processing so that Data Subjects are fully aware what, how and why their data is being processed;
- handle Personal Data only in ways defined by those notices, treating all Data Subjects equally;
- not process Personal Data in ways which would have unjustified adverse effects on the individuals concerned;
- not do anything unlawful with Personal Data.

(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. This means that staff will:

- document the lawful basis for processing in the University's Record of Processing Activity (ROPA);
- not further process Personal Data that has been obtained for a specific purpose for any incompatible purpose unless a further lawful basis has been identified. Each none-compatible, further processing activity will require a lawful basis before proceeding. If further processing is compatible with the original purpose and is identified in an existing privacy notice which has been circulated to subjects, no further action will be required.

(c) Personal Data shall be adequate, relevant and limited to what is necessary in relation to the processing purpose. This means that staff will:

- collect only enough Personal Data to satisfy the specified purpose;
- review datasets on an ongoing basis to use to ensure that fields of data that are not required, are removed;
- Ensure that when Personal Data is no longer required for specified purposes it is deleted or anonymised in accordance with the University's Records Management Classification Scheme and Records Retention Schedule.

(d) Personal Data shall be accurate and, where necessary, kept up to date. This means that staff will:

- take reasonable measures to ensure that Personal Data is accurate at the point of collection; this is of particular importance when data is obtained from any source other than the subject themselves, as there is a higher likelihood that errors may have been made;
- take reasonable steps to ensure data is up to date, such as periodically requiring data subjects to verify their contact details; and
- Act promptly upon any instructions from a Data Subject to amend inaccurate/changed personal data.

(e) Personal Data shall be kept in a form which permits identification of subjects for no longer than is necessary for the processing purpose. This means that staff will:

- consider opportunities to de-personalise records, where appropriate, throughout their life cycle where deletion is not appropriate; and
- follow the University Records Management Classification Scheme and Records Retention Schedule.

(f) Personal Data shall be processed securely and in a manner that protects against unauthorised or unlawful processing, loss, destruction or damage. This means that staff will:

- comply with the requirements of the University Information Security Policy and related regulations;
- apply security controls to the processing of data, appropriate to the nature and sensitivity of that data, paying particular caution to the processing of special category or criminal conviction data;
- take particular care when processing Personal Data at home or remotely as such processing presents an increased risk of loss, theft or damage to that data.

(g) The Data Controller shall be responsible for demonstrating compliance with the above principles. This means that staff will:

- comply with all University policies, codes of practice and guidance relating to Information Governance;
- if in doubt, seek advice from the Information Governance Team before processing Personal Data;
- promptly undertake all recommended and mandatory training programmes;
- highlight concerns about any activity that may compromise the security and privacy of Personal Data;
- comply with any request by the Information Governance Team to assess compliance with and/or effectiveness of Information Governance Policies, Codes of Practice and guidelines;
- When processing data about identifiable individuals, it may be appropriate to consider the distinction between ‘professional’ and ‘private’ data. For practical purposes, data relating to an individual’s professional capacity, e.g. University contact details or job title, will be subject to less stringent privacy considerations than data of a more private nature, e.g. home contact details;
- Prior to Personal Data being processed by another organisation on behalf of the University, the Information Governance Team must be consulted to ensure legislative compliance. In such cases, privacy impact assessments and contracts restricting use of Personal Data are likely to be required.

3. General requirements when processing special categories of data and criminal convictions data

Special Category data is defined as encompassing any Personal Data consisting of an individual’s race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sex life or sexual orientation.

Particular care must be taken with the processing of this category of Personal Data because of the greater potential impact to data subjects’ privacy rights, and greater consideration given to how to process the Data securely.

Criminal Convictions data is to be treated as particularly sensitive data and handled in accordance with the University's Criminal Convictions Policy.

4. Privacy Notices

As set out above, in accordance with the principle of transparency, Data subjects must be informed of the nature and purpose of processing Personal Data that will take place.

This will normally be achieved in the form of a privacy notice. Privacy notices are required regardless of the nature or format of collection of Personal Data whether via paper forms, online forms, information provided verbally, or other means. The aim of the notice is to ensure that any subsequent processing can be "reasonably expected" by the individual.

As a minimum the following information must be provided in a privacy notice:

- identity of the Data Controller (the University, not an individual or a department);
- contact details of the Data Protection Officer;
- purpose for processing;
- lawful ground for processing;
- any recipients of the data;
- length of time the Personal Data will be stored;
- if Personal Data is transferred abroad, the safeguards in place;
- use of any automated decision making (where relevant);
- details of data subjects rights, including the right to complain to the ICO;
- where the lawful basis is consent, the right to withdraw consent at any time; and
- where the lawful basis is contractual or statutory, the consequences of not providing the information.

The University publishes core privacy notices on its website describing the processing which takes place in respect of students, staff and general users of the website.

Specific privacy notices should be provided by all University services at the point of data collection, referring where appropriate to the General Privacy Notices.

If you are unsure whether a processing activity requires a privacy notice, or require assistance in wording a notice, please contact the Information Governance Team.

Where a privacy notice is supplied to an individual, a record of that notice should be kept for as long as the Personal Data is retained, plus six years (should a legal claim be brought against the University). Where a privacy notice is altered, previous versions must also be maintained in line with the above.

If a privacy notice changes it may need to be recommunicated to data subjects.

In certain circumstances it may be necessary to provide a privacy notice verbally but wherever possible this should also be provided in writing or documented in some way.

To support users in complying with the data protection principles when collecting Personal Data, a useful checklist is provided at Annex A.

5. Privacy By Design

It is important to minimise the unwarranted intrusions of privacy by designing systems which are robust and which ensure only data which is necessary for each specific purpose is processed and that technical and organisational measures are in place to ensure its security.

Where a project involves high risk processing a DPIA has to be carried out in accordance with the University's guidance on completing DPIAs. No processing may be carried out prior to this assessment being completed and the DPO authorising the processing.

You should conduct a DPIA in the following circumstances:

- The use of new technologies;
- Changing technologies (e.g.) programs, systems or processes;
- Automated processing or profiling
- Large scale systematic monitoring of a publicly accessible area
- Large scale processing in particular of special category data

A DPIA must include:

- A description of the processing and its purpose;
- The lawful basis for processing;
- An assessment of the necessity and proportionality of processing in this way;
- An assessment of the risks to individuals' privacy rights;
- Risk mitigation in place to minimise any potential impact on privacy rights.

6. Storage and disposal of Personal Data

Personal Data must always be kept appropriately secure against damage or unauthorised access, amendment or deletion, with precautions taken appropriate to its confidentiality and sensitivity in line with the University's Information Security Policy.

Electronic and physical files containing Personal Data should have appropriate access restrictions in place so that only authorised individuals can gain access to them.

Personal Data must not be stored on portable media devices (e.g. memory sticks, DVDs) unless approval of the Information Governance Team has been sought and appropriate safeguards put in place. There should be limited circumstances

where this is required because of the nature of the University's network and provision of secure, remote working options.

Where the processing of Personal Data on a portable media device has been authorised by the Information Governance Team, it must be encrypted using facilities provided by the University.

The use of hosted storage facilities (i.e. outside of the University's network) for Personal Data is not permitted unless:

- The system is controlled by the University; or
- Appropriate approval and advice has been sought from the Information Governance Team, usually requiring a privacy impact assessment and contract.

Personal Data must not be kept for longer than is necessary. Be particularly aware of electronic databases building up indefinitely. The University's Record Retention Schedule guides the retention requirements for records relating to various activities.

Personal Data must be disposed of in a manner appropriate to its sensitivity. Records awaiting destruction must continue to be stored securely.

The Confidential Waste Units (CWU) placed around site must be used for the destruction of paper Personal Data. All units are completely emptied on a regular and auditable basis within recommended confidential waste industry timescales. Units are emptied by Contractor staff on a scheduled basis. Extra bags and boxes should be removed at the same time. Paper waste that does not contain Personal Data may still be considered confidential, such as none published corporate or unit plans, financial information and anything that may have a negative commercial impact on the business if made available to unauthorised individuals. Confidential paper data must also be disposed of via these units.

Paper data that is not personal and not confidential should be placed in waste paper bins but if there is any uncertainty as to the confidentiality of paperwork it is best to err on the side of caution and use the CWU.

7. Disclosure and sharing of Personal Data with Third Parties

Personal Data may not be disclosed to any third party without the consent of the individual concerned or a defined and documented lawful basis for sharing. In this context "third parties" includes, but is not limited to, family members, friends, local authorities, government bodies and the police.

Requests for the disclosure of Personal Data must be referred to the Information Governance Team so that a lawful basis for sharing the information can be demonstrated. The exceptions to this are:

- cases where the immediate disclosure of Personal Data is required by law enforcement or health care agencies for the imminent prevention of serious crime or the prevention of significant harm to an individual and advice from the Information Governance Team is unavailable (e.g. outside

of standard working hours). Staff must take reasonable steps to verify the identity of the requestor, disclose only what is immediately necessary and document the details of the disclosure including the requestor contact details, purpose of request and information disclosed;

- cases where schools or departments have been authorised by the Information Governance Team to routinely handle disclosures directly, in which case specific procedures will be agreed.

The provision of references is the subject of a separate University policy.

Personal Data can be shared within the University provided that such sharing is reasonable, necessary, not excessive, and is not incompatible with the original purpose for gathering the data.

When disclosing or discussing information about individuals, reasonable steps should be taken to verify the identity of the recipient, especially in telephone conversations or email correspondence. No information should be provided without a lawful basis for disclosing the information. Be aware of the risk of individuals posing as apparently legitimate recipients in order to acquire information from the University.

When disclosing or sharing Personal Data, particular care must be given to the risks of correspondence being intercepted or errors in transmission. Only the minimum necessary information should be included and particular care must be taken when entering the recipient's details. If appropriate to the sensitivity of the information, email attachments can be password protected and/or encrypted.

8. Data Subject Rights Request

Data Subjects have a right to be informed of the Personal Data processed by the University about them. This is commonly known as a data subject access request or SAR.

From 25th May 2018, such requests can be made free of charge, by any means of contact (including by telephone) and must be completed within one calendar month, or four calendar months in exceptional cases.

Data subjects wishing to exercise this right should be directed to place their request in writing to dpo@tees.ac.uk or call 01642 342093 / 01642 342563.

Any request directed to an individual member of staff must be directed to the Information Governance Team without delay.

The Information Governance Team will co-ordinate all requests for access to Personal Data, with the assistance of the school or department responsible for the information.

9. Personal Data Breaches

A Personal Data breach is considered to be any loss, damage or destruction to Personal Data or the unauthorised access, disclosure and/or processing of Personal Data.

Such incidents may cause unwarranted damage or distress to data subjects, generate negative media attention and/or constitute a breach of Data Protection Law for which the University can be subject to financial penalties of up to 20 million Euros or 4% of annual global turnover.

Examples of Personal Data breaches include:

- Loss or theft of devices or equipment on which Personal Data is stored e.g. a memory stick;
- An email containing Personal Data sent to the wrong person;
- Disclosure of Personal Data, via any method, to a third party such as a family member without consent or another legal power or obligation to do so; and
- A member of staff who has accessed the personal records of family or friends without their consent.
-

The GDPR includes a requirement to report significant breaches within 72 hours.

To ensure that breaches can be investigated and managed with the legislative timeframes they must be reported to the Information Governance Team in Legal & Governance Services without delay via dpo@tees.ac.uk or tel ext. 2093 or 2563. Reference is to be made to the University's Data Breach Management Policy.

10. Complaints

Any complaints, concerns or dissatisfaction regarding the University's processing of Personal Data must immediately be brought to the attention of the Data Protection Officer (Legal & Governance Services).

11. Contacts and Further Information

Queries relating to the processing of Personal Data or the Data Protection Act 2018 should be referred to the Information Governance Team email: dpo@tees.ac.uk; tel. ext. 2093 or 2563. Additional guidance is also accessible from the Legal & Governance Services intranet available here.

Annex A

Personal Data Processing Checklist

This checklist should be used whenever there are plans to collect Personal Data for the first time or in respect of processing activities that are not already routinely carried out by the University.

Consideration	**YES NO N/R**	**Details / Justification**
Is it *necessary* to collect this data?		
Have I checked there will be no unjustified adverse effects on data subjects as a result of this processing?		
Has the use of anonymised/pseudonymised data been considered instead?		
Has a privacy notice been provided to the data subject? (describe how)		
Is any potential further processing covered in the above?		
Has an Article 6 lawful basis been identified?		
Has an Article 9 lawful ground been identified (only if special category data)		
Is the activity recorded in the University's Record of Processing Activity?		
Have reasonable steps been taken to ensure the accuracy of the data?		
Will the data be processed securely?		
If the data will be shared with others, does the subject know to expect that?		
If a third party will process this data on the University's behalf, is there a contract in place that has been approved by Legal & Governance Services?		
Do you know how long to keep the data for?		

If you have answered no to any of the above questions, contact the Information Governance Team before proceeding.