University of Sunderland
Technical Services
Cyber Security and Information Governance
Policy Document
Classification – Public

Data Protection Policy	
Version Number:	V1.0
Policy Reference:	
Policy Owner:	Data Protection Officer
Date Written:	January 2018
Date of Last Update:	N/A
Author:	Information Governance Manager and Data Protection Officer
Approval Route:	Tech Services > Operations Board
Date Approved:	March 2018
Next Review:	January 2020
Comments:	Complete rewrite of the DP Policy to account for GDPR

1. INTRODUCTION AND PURPOSE

1.1. The University of Sunderland needs to gather and use certain information about individuals. This can include enquirers, applicants, students, staff and other third parties the University has a relationship with or may need to contact. On this basis, the University of Sunderland is a data controller (ICO registration number Z6120473). This policy describes how this personal data must be collected, handled and stored to meet the requirements of the General Data Protection Regulations (GDPR).

1.2. This policy ensures that the University of Sunderland:

- Complies with the principles of the GDPR, and any subsequent laws which are passed within England and Wales.
- Protects the rights of those individuals which the University of Sunderland, collects, handles and stores information on.
- Is open about how it stores and handles individuals' data
- Protects itself from the risk of data breach.

1.3. The GDPR describe how organisations, including the University of Sunderland, must collect, handle and store personal information. These rules apply regardless of whether the data is stored electronically, on paper or on other media. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. The GDPR is underpinned by 6 important principles. These say that personal data must:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency**');
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('**purpose limitation**');
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**');
- Accurate, and where necessary, kept up to date ('**accuracy**');
- Kept in a form which permits identification of data subjects for no longer than in necessary for the purposes for which the personal data are processed ('**storage limitation**'); and
- Processed in a manner that ensures appropriate security of the personal data ('**integrity and confidentiality**').

The full principles of data processing from the GDPR can be found in Appendix 1.

2. SCOPE

2.1. This policy applies to:

- The University of Sunderland;
- All subsidiary companies of the University of Sunderland;

- All staff of the University of Sunderland and its subsidiary companies;
- All contractors, suppliers and other people working on behalf of the University of Sunderland or its subsidiary companies.

2.2. It applies to all data that the University of Sunderland holds in relation of any identifiable individuals.

3. DEFINITIONS

3.1. **Personal Data** means any information relating to an identified or identifiable natural living person ('data subject'); an identifiable natural personal is one who can be identified, directly or indirectly, in particular by reference to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.2. **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.

3.3. **Data controller** means any individual or organisation which either alone or jointly, determines the purposes and means of the processing of personal data.

3.4. **Data Processor** means any individual or organisation which processes personal data on behalf of a controller

3.5. **Personal data breach** means a breach of security or process leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

4. ROLES AND RESPONSIBILITIES

4.1. Everyone who works for or with the University of Sunderland and its subsidiary companies has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and GDPR principles. It is important to note that a breach in this policy could lead to disciplinary proceedings and a significant fine (up to €20 million) for the University of Sunderland.

4.2. The **Board of Governors** is ultimately responsible for ensuring that the University of Sunderland and its subsidiary companies meets its legal obligations.

4.3. The **Data Protection Officer** is responsible for:

- Informing and advising the organisation and its employees of their data protection obligations under the GDPR
- Monitoring the organisation's compliance with the GDPR and internal data protection policies and procedures. This will include monitoring the assignment of responsibilities, awareness training, and training staff involved in processing operations and related audits.

- Advising on the necessity of data protection impact assessments (DPIAs), the manner of their implementation and their outcomes.
- Serving as the contact point to the data protection authorities for all data protection issues, including data breach reporting.
- Serving as the contact point for individuals (data subjects) on privacy matters, including subject access requests.

4.4. The **Cyber Security Architect**, is responsible for:

- Developing technical security standards to be used across the University of Sunderland technical estate.
- Ensuring teams across the University carry out regular checks and scans to ensure security hardware and software is functioning properly
- Evaluating the technical security arrangements of any third-party services the University of Sunderland is considering using to store or process data, using a Supplier Information Security Assessment to gather evidence.

5. POLICY DETAILS

5.1. The University will comply with the principles of the General Data Protection Regulations (see Appendix 1 of this document) when processing any personal data.

5.2. The University will only process personal data where it can match processing activities to one or more of the lawful bases for processing under Article 6(1) of the GDPR (See Appendix 2) or in the case of special category personal data Article 9(1) of the GDPR (See Appendix 3).

5.3. The University will ensure that a record of the processing activity it undertakes is maintained (as required by the GDPR) and made available to the relevant authority (the ICO in the UK), upon request.

5.4. The University will ensure that all new and significantly amended systems are subject to sufficient Data Privacy Impact Assessment (DPIA) assessment, and the risks identified are appropriately managed. For internal processes or systems this will be in the form of a Privacy Impact Assessment (PIA) and where there is the involvement of an external partner (data processor) who will handle or store information on behalf of the University a Supplier Information Security Assessment (SISA) will be used to assess their technical security arrangements.

5.5. By default, the minimum information classification (please see information classification process) which will be used for records containing personal data will be restricted, and for those records containing special category data confidential, and the controls outlined in the information classification will be followed.

5.6. The University will ensure that all requests made by data subjects in accordance with the GDPR are handled appropriately and within the prescribed time limits (30 calendar days, from receipt of sufficient evidence of identity, for Subject Access Requests). Where requested to do so, the University will also advise the data

subject of the purposes for which the data are to be processed and the recipient or classes of recipients to which the data are or may be disclosed (please see guidance document handling requests from information).

5.7. In the event of a personal data breach the University will use a managed, documented approach to managing the incident including assessing the severity of the incident, and where applicable will notify the ICO within 72 hours of becoming aware of the incident (please see guidance document (Handling Data Breaches Guide).

6. TRAINING AND EDUCATION

6.1. All staff and contractors of the University of Sunderland and its subsidiary companies who do or are likely to come into contact with personal data in carrying out their responsibilities are required to receive Data Protection Training, on this basis the University will:

- Ensure that all new staff and contractors of the University and its subsidiary companies receive appropriate Cyber Security and Data Protection training as part of their induction, and that, until such training has been undertaken, access to systems and storage media containing personal information will be prohibited.
- Ensure that all existing staff and contractors of the University and its subsidiary companies undertake appropriate Cyber Security and Data Protection training, which will be refreshed on a yearly basis. Staff who fail to undertake this training will have their IT account suspended, and thus their access to personal information will be revoked until training is complete.

6.2. This policy will come into effect on the 25th May 2018 when the General Data Protection Regulations and any associated law in England and Wales are in place and enforceable.

6.3. This policy will be uploaded to the policy management tool and will be delivered to staff desktops to ensure awareness, staff will be required to 'click' to advise they have read the policy and understood its contents, this will take place in May 2018, and then be redelivered on a yearly basis.

6.4. This policy will be uploaded to the Technical Services website along with all associated processes, procedures and guidance notes.

7. DOCUMENTS

7.1. All staff should also be aware of the following policies:

- Information Security Policy
- Document and Record Management Policy

7.2. All staff should be aware and where applicable follow the processes and procedures outlined in the following documents:

- Information Classification Process
- Data Protection by Design handbook
- Creation and management of Privacy Notices
- Processing student information – Legal Bases
- Processing staff information – Legal Bases
- Handling Requests for information
- Handling Data Breaches Guide
- Right to be forgotten, data portability and inaccuracy correction staff guidance document
- Dealing with Data Protection complaints
- University of Sunderland Retention Schedule
- Sharing personal information with others
- Guide on the use of personal data in research

Appendix 1 - GDPR PRINCIPLES

1. There are 6 processing principles in the GDPR, in full they are:
   Personal data shall be:
   - Processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency);
   - Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')
   - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
   - Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')
   - Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
   - Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

Appendix 2 – LAWFUL BASES FOR PROCESSING PERSONAL DATA

1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:
    a. The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
    b. Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
    c. Processing is necessary for compliance with a legal obligation to which the controller is subject;
    d. Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
    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 controller;
    f. Processing is necessary for the purposes of the legitimate interests pursued by the controller or third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) shall not apply to processing carried out by public authorities in performance of their tasks.

Appendix 3 – LAWFUL BASES FOR PROCESSING SPECIAL CATEGORY PERSONAL DATA

1. Processing of personal data 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 shall be prohibited, unless one of the following applies:
    a. The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
    b. Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subjects;
    c. Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally in capable of giving consent;
    d. Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
    e. Processing relates to personal data which are manifestly made public by the data subject;
    f. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
    g. Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
    h. Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care system and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 2;
    i. Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for

suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

2. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another personal also subject to an obligation of secrecy under Union or Member State law or rule established by national competent bodies.

Version History

Version Number	Date	Description	By
V0.1	January 2018	Initial version written	Info Gov Manager
V0.2	March 2018	Small changes made to overall policy	Info Gov Manager
V0.3	March 2018	Changes to take account of comments received from Deputy Director Technical Services	Info Gov Manager
V0.4	March 2018	Changes to take account of comments received from Cyber Security Architect	Info Gov Manager
V1.0	March 2018	Policy approved	Operations Board