Data Protection Policy

Policy No.
Effective Date: May 25th 2018
Last Revised: March 2018
Review Date: May 25th 2019
Approval Body: University Management Board

Prifysgol Abertawe
Swansea University

Policy Owner: Registrar, Swansea University
Policy Author(s): Bev Buckley, Data Protection Officer
Gail Evans, IT Policy Lead

1. Definitions

Term	**Definition**
Personal Data	Data relating to a living individual who can be identified from the data, or from the data and other information which is in the possession of (or likely to come into the possession of) the Data Controller and includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual.
Special Category Personal Data	Special Category Personal Data is personal data revealing an individual's racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying and individual, data concerning physical or mental health (including disabilities) or sexual life or sexual orientation.
Data Controller	The Data Controller is a person or organisation who determines the purposes for which, and the manner in which, any personal data are, or are to be, processed. For the purposes of this policy, the University is the registered Data Controller.

Data Processor	The Data Processor is any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller e.g. a person or organisation that collects and processes data on behalf of the University under contract.
Processing	Data Processing is any operation on personal data, including obtaining, recording, holding, organising, adapting, combining, altering, retrieving, consulting, disclosing, disseminating, deleting, destroying and otherwise using the personal data.
Data Subject	The Data Subject is a living individual who is the subject of the personal data.
Consent	Valid Consent is any freely given, specific, informed and unambiguous indication of the individual's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of personal data relating to them.
Third Party	A Third Party is any person other than the Data Subject, the Data Controller or any Data Processor or person authorised to process data for the Data Controller or Data Processor.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise Processed.
Privacy Notice	Data protection laws require the Data Controller to provide detailed, specific information to the Data Subject about how and why their personal data is being processed (including the identity of the Data Controller and the Data Protection Officer, how and why the University will use, process, disclose, protect and retain that personal data). Such information must be provided through appropriate Privacy

	Notices. Privacy Notices should be provided at the point of collection of personal data and ideally via the same medium. The Data Subject should be notified of any change to a Privacy Notice. Given the level of engagement with external parties and industries, and the different programmes the University have ongoing, this may require regular review and management. Further information on Privacy Notices can be found on the Information Commissioner's Office website:- http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_notices

2. Background

The General Data Protection Regulation (GDPR) will apply in the UK and the rest of the EU from 25 May 2018 and will replace the Data Protection Act 1998 (DPA). The GDPR is designed to harmonise and strengthen data protection law and practice across the EU. Like the DPA, it will be regulated in the UK by the Information Commissioner's Office (ICO).

It will apply in the UK and is supplemented in by a Data Protection Bill that was introduced in Parliament in September 2017 and will become law by May 2018; amongst other things, the Bill legislates in those areas where the GDPR gives EU Member States the discretion to vary the rules, and it sets out the ICO's regulatory powers in more detail.

Like the DPA, the GDPR sets out rules and standards for the use of information about living identifiable individuals and applies to all organisations in all sectors, both public and private. It doesn't apply to anonymous information or to information about the deceased. The GDPR's rules and standards are based around the existing DPA concepts of data protection principles and individual rights. Accordingly, many of the concepts in the GDPR and reflected in this document are updated from current provisions in the DPA.

3. Purpose

Swansea University holds personal data about job applicants, employees, workers, students, suppliers and other individuals for a variety of purposes.

This policy sets out how the University seeks to protect personal data and ensure staff and students understand the rules governing their use of personal data to which they have access in the course of their work and/or studies.

4. Scope

The policy applies to all staff and students, and all items of personal data that are created, collected, stored and/or processed through any activity of Swansea University, across all areas including Schools, Colleges, Professional Services Units as well as wholly owned subsidiaries.

The policy covers, but is not limited to, Cloud systems developed or commissioned by Swansea University, any systems or data attached to University data or telephone networks, systems managed by Swansea University, mobile devices used to connect to the University networks or which hold University data, data over which Swansea University holds the intellectual property rights, data over which Swansea University is the data controller or data processor or electronic communications sent from Swansea University.

5. The Data Protection Principles

Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- kept safe and secure

In addition to the above principles, the University must also be able to demonstrate compliance with data protection legislation. This is commonly known as the 7th Data Protection principle.

Further guidance on the data protection principles is described in Appendix 1.

6. Conditions of Processing and Consent

In order for it to be legal and appropriate for the University to process personal data, at least one of the following conditions must be met:

- The data subject has given his or her consent
- The processing is required due to a contract
- It is necessary due to a legal obligation

- It is necessary to protect someone's vital interests (i.e. life or death situation)
- It 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.
- It is necessary for the legitimate interests of the controller or a third party and does not interfere with the rights and freedoms of the data subject (this condition cannot be used by public authorities in performance of their public tasks). It should be noted that under GDPR, universities are classified as public authorities and therefore the use of the 'legitimate interests' justification is not possible in terms of Swansea University's *core activities*. It may be possible to use legitimate interests for processing that is undertaken *outside the University's core activities*.

All processing of personal data carried out by the University must meet one or more of the conditions above. There is stronger legal protection for more sensitive information, such as ethnic background, political opinions, religious beliefs, health, sexual health or criminal records. The Vice Chancellors Office can provide further advice on processing sensitive information.

Consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement or other clear affirmative action, signifies agreement to the processing of personal data relating to him or her". The GDPR clarifies that silence, pre-ticked boxes or inactivity does not constitute consent.

Anyone who has provided consent has the right to revoke their consent at any time.

The Data Protection Officer can provide further advice on obtaining consent.

7. The Rights of an Individual

The University will ensure that personal data is processed in accordance with the rights of Data Subjects under data protection law. An individual has the right to:

- receive certain information about the University's processing activities in a Privacy Notice (see **Appendix 2**)
- request access to their personal data that the University holds, via a subject access request
- ask the University to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed
- rectify inaccurate data or to complete incomplete data
- restrict processing in specific circumstances

- in limited circumstances, receive or ask for their personal data to be transferred to a Third Party in a structured, commonly used and machine-readable format
- withdraw Consent to Processing at any time
- prevent the University's use of their personal data for direct marketing purposes
- to challenge processing which has been justified on the basis of the University's legitimate interests or in the public interest
- request a copy of an agreement under which personal data is transferred outside of the EU
- object to decisions based solely on automated processing, which produces legal effects or significantly affects an individual
- prevent processing that is likely to cause damage or distress to the individual or anyone else
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedom.
- make a complaint to the supervisory authority

Automated Processing and / or Decision Making

Staff must contact the Data Protection Officer and a DPIA must be carried out before any automated processing (including profiling) or automated decision-making activities are undertaken. Please see **Appendix 2** for further guidance.

8. The Accountability of the University

The GDPR is more prescriptive than the DPA about how organisations need to implement the above provisions and it also introduces a range of accountability requirements to encourage a proactive and documented approach to compliance.

Swansea University will:

- appoint a Data Protection Officer
- implement policies, procedures, processes and training to promote 'data protection by design and by default'
- have appropriate contracts in place when outsourcing functions that involve the processing of personal data
- maintain records of the data processing that is carried out across the organisation
- document and report personal data breaches
- carry out Data Protection Impact Assessment on 'high risk' processing activities

Further guidance on these areas is described in **Appendix 2**.

9. Policy Statements

Lawful processing of personal data is vital to the successful operation and reputation of Swansea University, and for maintaining the trust of our students, employees and other stakeholders. It is a critical responsibility that we take seriously at all times. The University is committed to protecting the rights and freedoms of individuals in accordance with the provisions of data protection legislation. In order to achieve this, the University shall ensure that personal data is handled appropriately and consistently.

The University is responsible for demonstrating compliance with the data protection principles. Compliance with the GDPR, and adhering to these principles is the responsibility of all members of the University.

The University collects personal data in the course of registering students, employing staff or providing services to customers. The University has to satisfy at least one of the conditions in the Act for the processing of personal data and ensure that the processing is fair.

All University users of personal data must ensure that all personal data they hold is kept securely. They must ensure that it is not disclosed to any unauthorised third party in any form, either accidentally or otherwise.

Cloud based services store information on servers that don't belong to the University, so it is important that users ensure that cloud services are compliant with University data protection and information security policies.

Individual areas within the University are responsible for ensuring the appropriate retention periods for the information they hold and manage, based on University Guidance (to be developed). Retention periods will be set, based on legal and regulatory requirements, sector and best practice guidance. A useful source of guidance is available at the JISC Higher Education Business Classification Scheme and Records Retention Schedules.

Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. Once information is no longer needed it should be disposed of securely. Paper records should be shredded or disposed of in confidential waste and electronic records should be permanently deleted. If data is fully anonymized then there are no time limits on storage, from a data protection point of view.

Consent should be obtained using an ‘opt-in’ by the data subject rather than an ‘opt-out’. This means that the University will not assume consent has been given simply by the absence of an objection.

Individuals providing their personal data to the University should be aware who the data controller is and what will be done with their data. Appropriate 'collection notices' or 'fair processing notices' will need to be provided. Advice can be sought from the Data Protection Officer if necessary.

The University will manage the personal data it processes in a secure way. This applies to paper and electronic records systems. Systems should be access controlled, staff appropriately trained and security processes should be developed and understood. Appropriate monitoring and reporting on data security risks, initiatives and developments will be undertaken by the University's management groups.

In the event that the University engages a third party as a 'data processor' for its personal data, a specific written contract with the supplier providing assurance of security provision will be in place. The University will not rely on supplier set 'terms and conditions'.

The University will consider the impact on data privacy during all processing activities. This includes implementing appropriate technical and organisational measures to minimise the risk to personal data.

The University will implement privacy by design when Processing personal data by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with data privacy principles.

Transfers of Personal Data Outside the EU

Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The GDPR lists the factors that should be considered to ensure an adequate level of protection for the data and some exemptions under which the data can be exported.

Information published on the internet must be considered to be an export of data outside the EU. This covers data stored in the cloud unless the service provider explicitly guarantees data storage only takes place within the EU.

The Information Commissioner's Office Guidance on the use of Cloud Computing should be consulted before any use of external computing resources or services via a network which may involve personal data.

Staff involved in transferring personal data to other countries should consult the Data Protection Officer.

Further guidance can be found in **Appendix 1**.

Direct Marketing

Direct marketing relates to the communication, regardless of the media employed, which directs advertising or marketing materials to individuals e.g. mail shots for fund raising, advertising courses etc.

Individuals must be given the opportunity to remove themselves from lists or databases used for direct marketing purposes. The University must cease direct marketing activity if an individual requests the marketing to stop.

Direct marketing must also comply with the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) which covers marketing via telephone, text and email. For more information about direct marketing and PECR please see the Data Protection Guidance. The Privacy and Electronic Communications (EC Directive) Regulations 2003 is due to be replace by a new ePrivacy Regulation in 2018.

10. Records of Processing Activities

As a data controller, the University is required to maintain a record of processing activities which covers all the processing of personal data carried out by the University. Amongst other things, this record contains details of why the personal data is being processed, the types of individuals about which information is held, who the personal information is shared with and when personal information is transferred to countries outside the EU.

11. Children

Under GDPR the following restrictions apply to the processing of personal information relating to children:

- Online services offered directly to children require parental consent

- Any information provided to a child in relation to their rights as a data subject has to be concise, transparent, intelligible and easily accessible, using clear and plain language

- The use of child data for marketing or for profiling requires specific protection

The Data Protection Officer should be informed if any of the above activities are being contemplated.

12. Research

The GDPR adopts a "broad" definition of research, encompassing the activities of public and private entities alike. The GDPR aims to encourage innovation, as long as organisations implement appropriate safeguards. It is important that staff collecting data for research purposes process the data in line with the GDPR and University guidance.

13. Data Sharing

Certain conditions need to be met before personal data can be shared with a third party or before an external data processor is used to process data on behalf of the University.

As a general rule, personal data should not be passed on to third parties, particularly if it involves special categories of personal data but there are certain circumstances when it is permissible.

- Any transfers of personal data must meet the data processing principles, in particular it must be lawful and fair to the data subjects concerned (see **Data Protection Principles** above)
- It must meet one of the conditions of processing (see **Conditions of Processing and Consent** above).

Legitimate reasons for transferring data could include:

- a legal requirement
- necessary for the official core business of Swansea University
- if no other conditions are met, then consent must be obtained from the individuals concerned and appropriate privacy notices provided (see **Appendix 2**)
- the University is satisfied that the third party will meet all the requirements of GDPR, particularly in terms of holding the information securely

Where a third party is processing personal data on behalf of the University, a written contract must be in place. A contract is also advisable when data is being shared for reasons other than data processing so the University has assurances that GDPR requirements are being met.

Staff should consult with the Data Protection Officer if they are entering into a new contract that involves the sharing or processing of personal data.

Staff who receive requests for personal information from third parties such as relatives, police, local councils etc. should consult the Data Protection Officer.

14. Data Protection Breaches

The University will make every effort to avoid Personal Data Breaches and in particular the loss of personal data. However, it is possible that mistakes will occur on occasion. What is important in these circumstances is that the University responds appropriately in accordance with the data protection laws.

The data protection laws require the University to notify Personal Data Breaches to the relevant supervisory authority (for our purposes, this will usually be the Information Commissioner's Office) 72 hours after first becoming aware of the incident and to the individual Data Subjects, in certain circumstances.

Staff should be aware that a failure to notify Personal Data Breaches to relevant supervisory authorities and Data Subjects in accordance with the requirements of the data protection laws may lead to fines of up to €10million or 2% of annual global turnover (whichever is the highest).

If staff know or suspect that a Personal Data Breach has occurred, they should not attempt to investigate the matter themselves. The University has a Personal Data Breach Reporting Procedure in place. Staff should be familiar with this procedure and immediately contact ISS in the event of a personal data breach in accordance with that procedure.

15. Responsibilities of Staff

All staff, who have responsibilities for the collection, access or Processing of Personal Data, should comply with the provisions of the applicable data protection laws in accordance with the principles outlined 0 above.

Line managers are required to make sure staff members are aware of the applicable data protection laws and the University's Data Protection Policy and seek out additional guidance and training via the Data Protection Officer.

All staff are responsible for ensuring that any personal data that they provide to the University in connection with their employment is accurate and up to date.

It is a condition of employment that all employees abide by the Data Protection Policy and failure to do so may therefore result in disciplinary action.

16. Responsibilities of Students

Students are required to ensure that where they provide their own personal data to the University, it is accurate and up-to-date.

Students must comply with the University's **Acceptable Use of IT Facilities and Systems Policy**. Failure to do so may therefore result in disciplinary action.

17. Data Protection Support

The Data Protection Officer is responsible for the day-to-day data protection queries and requests such as subject access requests, and is a point of contact for issues relating to data protection. The Data Protection Officer is also responsible for producing guidance on good data protection practice and in promoting compliance across the University. The Data Protection Officer will also provide training to individuals/groups upon request or where a need has been identified.

18. Related Policies

Title	Link
Information Security Consultancy – Security Policy	http://www.swansea.ac.uk/media/InformationSecurityPolicy%20June%202015.docx
Acceptable Use of IT Facilities and Systems Policy	TBA

19. Consequences of a Breach

Any breach of the policy may result in the University, as the Data Controller, being liable in law for the consequences of the breach. In addition, breach of this policy by staff or students may be considered to be a disciplinary offence and may be dealt with according to the University's disciplinary procedures. Failure to comply with this policy may result in disciplinary action up to and including termination of employment or studies.

20. Policy History

Revision Date	Author	Description

Appendix 1

The Seven Data Protection Principles

(a) **Principle 1 - Personal Data must be processed lawfully, fairly and in a transparent manner**

The University will ensure that data is obtained fairly and in a transparent manner by providing a Privacy Notice to Data Subjects either at the point of collection where the personal data is collected directly from the Data Subject, or at the first communication with the Data Subject or within 1 month of receiving the personal data (whichever is earlier) where the personal data are received from a Third Party.

The Privacy Notice will set out about how and why their personal data is being processed (including the identity of the Data Controller and the [Data Protection Officer], how and why the University will use, process, disclose, protect and retain that personal data) and will be concise, transparent, intelligible, easily accessible, and in clear and plain language so that Data Subjects can easily understand it (see separate guidance on Gathering Personal Data)

Information about how the University processes data relating to students is contained within the Student Privacy Notice. This explains to students what personal data the University collects about them, how their data will be used by the University, with whom their data may be shared with and what their rights and responsibilities are in regard to their data.

In order for Processing to be lawful, personal data (which is not Special Category Personal Data) will only be processed by the University if one of the following conditions, has been met:

(i) The Data Subject has given his or her Consent;

(ii) The Processing is necessary for the performance of a contract between the University and the Data Subject;

(iii) To meet the University's legal compliance obligations;

(iv) To protect the Data Subject vital interests;

(v) For the performance of a task in the public interest;

(vi) To pursue the University's legitimate interests, where these interests are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of the Data Subject(s). The purposes for which the University Processes personal data for legitimate interests (if applicable) need to be set out the Privacy Notices.

(The use of the Legitimate Interests condition can only be applied where processing does not fall within the University's core function).

The Processing of Special Category Personal Data is prohibited unless an alternative legal basis for Processing is met. Processing of Special Category Personal Data will only be carried out by the University if one of the following applies:

(i) The Data Subject has given his/her explicit Consent.

(ii) The Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or the Data Subject in the field of employment and social security and social protection law.

(iii) The Processing is necessary to protect the vital interests of the Data Subject or another person.

(iv) The 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 and 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;

(v) The Processing relates to personal data which has been made public by the Data Subject.

(vi) The Processing is necessary for the establishment, exercise or defence of legal claims.

(vii) The Processing is necessary for reasons of substantial public interests on the basis of UK law.

(viii) The 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 management of health or social care systems and services.

(ix) Processing is necessary for reasons of public interest in the area of public health.

(x) Processing is necessary for archiving purposes in the public interests, scientific or historical research purposes or statistical purposes provided that the Processing is proportionate to the aim pursued, respects the essence of the right to data protection and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject.

(b) **Principle 2 - Personal Data will be held for specified, explicit and legitimate purposes and must not be further processed in a manner incompatible with that purpose or purposes for which they are processed**.

The University will ensure that personal data which is obtained for a specified purpose is not used for different or incompatible purposes from those disclosed when the personal data was first obtained, unless the Data Subjects have been informed of the new purposes and legal basis being relied upon (if this legal basis is Consent, appropriate Consent must be obtained).

(c) **Principle 3 - Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purpose or purposes for which they are processed**

The University will ensure that it collects only the minimum personal data necessary for the purpose or purposes specified and will not collect or hold data on the basis that it might be useful in the future.

(d) **Principle 4 - Personal Data shall be accurate and, where necessary, kept up to date**

The University will take reasonable steps to ensure the accuracy of personal data which it holds, and will take steps to amend, update or correct inaccurate data when requested to do so by a Data Subject. personal data will be inaccurate where it is incorrect or misleading as to any matters of fact.

(e) **Principle 5 - Personal Data processed for any purpose shall not be kept for longer than is necessary for that purpose**

The University will ensure that personal data is not kept for longer than is required by the purpose or purposes for which the personal data was gathered.

Staff must ensure that personal data is securely destroyed once the purpose or purposes for Processing has come to an end and there is no legal requirement or valid operational reason for its continued retention (see separate guidance on Retaining Personal Information).

The University may retain certain personal data indefinitely for research purposes (including historical or statistical purposes) as permitted under the data protection law (see separate guidance on the use of personal data in research).

(f) **Principle 6 - Appropriate technical and organisational measures shall be taken to prevent the unauthorised or unlawful processing of Personal Data and the accidental loss, destruction of, or damage to, Personal Data**

The University will take reasonable and appropriate steps to ensure the security of personal data which are held electronically and in manual form, to prevent unlawful or unauthorised Processing of personal data and against the accidental loss of, or damage to, or destruction of personal data. Please see additional information on data security for specific guidance.

The University will take reasonable and appropriate steps to maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(i) Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

(ii) Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

(iii) Availability means that authorised users are able to access the personal data when they need it for authorised purposes.

The University will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of personal data

(g) **Principle 7 – The Data Controller shall be responsible for, and able to demonstrate compliance with the other data protection principles (the accountability principle).**

The University will ensure that appropriate technical and organisational measures are implemented to ensure compliance with data protection principles

The University will have adequate resources and controls in place to ensure and to document data protection law compliance including:

(i) Appointing a suitably qualified DPO

(ii) Implementing data protection by design and default when Processing personal data to ensure compliance with applicable data protection laws.

(iii) Completing Data Protection Impact Assessments (DPIAs) to identify and reduce risks of a data Processing activity, where Processing presents a high risk to rights and freedoms of individuals. DPIAs should be conducted for all major system or business change programs involving the Processing of personal data particularly those involving new initiatives or technology.

(iv) Integrating data protection into internal documents, policies and procedures including this Data Protection Policy;

(v) Regularly training staff on applicable data protection law, this Data Protection Policy, related policies and guidelines and data protection matters including, for example, individual rights, Consent, legal basis, DPIAs and Personal Data Breaches; and

(vi) 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.

Limitations on transfers of Personal Data outside the European Union (EU)

Data protection law restricts data transfers to countries outside the European Union, to third countries or international organisations in order to ensure that the level of data protection afforded to individuals is not undermined. Personal Data is transferred from the originating country across borders when it is transmitted, sent, viewed or access in a different country.

Personal Data should only be transferred the EU if one of the following conditions applies:

- The European Commission has issued a decision confirming that the country to which the Personal Data is transferred ensures an adequate level of protection for the individuals' rights and freedoms (an 'adequacy decision').
- The Personal Data is transferred under the EU-US Privacy Shield.
- Appropriate safeguards are in place. Adequate safeguards may be provided for by:
    - a legally binding agreement between public authorities or bodies;
    - binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
    - standard data protection clauses in the form of template transfer clauses adopted by the Commission;
    - standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
    - compliance with an approved code of conduct approved by a supervisory authority;
    - certification under an approved certification mechanism as provided for in the GDPR;
    - contractual clauses agreed authorised by the competent supervisory authority; or
    - provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

Further information about the European Commission's list of approved countries and the standard contractual clauses is available on the Information Commissioner's Website https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/

Data protection law also contains a number of exemptions to the limitations on transfers of Personal Data outside the EU (regardless of the country to

which the Personal Data are transferred or the receiving organisation). The exemptions are as follows:

- The Data Subject has given his/her explicit Consent to the transfer after having been informed of the possible risks of such transfers due to the absence of an adequacy decision and appropriate safeguards.
- The transfer is necessary for the performance of a contract between the Data Subject and the University or the implementation of pre-contractual measures taken at the Data Subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the University and Third Party.
- The transfer is necessary for important reasons of public interest.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the Data Subjects or other individuals.
- The transfer is part of Personal Data on a public register.

As the University is a public authority, the availability of the exemptions outlined in (a), (b) and (c) above are limited.

Further guidance should be sought from the Data Protection Officer in relation to transferring of Personal Data outside the EU.

Appendix 2

Privacy Notices
Under the 'fair and transparent' requirements of the first data protection principle, the University is required to provide data subjects with a 'privacy notice' to let them know what it does with their personal data.

Privacy notices are published on the University website and are therefore available to staff and students from their first point of contact with the University. Any processing of staff or student data beyond the scope of the standard privacy notice, or processing of the personal information of any other individuals will mean that a separate privacy notice will need to be provided.

Further information on what information should be included in a privacy notice is provided in the Data Protection Guidance.

Data Protection by Design
Under the GDPR the University has an obligation to consider the impact on data privacy during all processing activities. This includes implementing appropriate technical and organisational measures to minimise the risk to personal data.

It is particularly important to consider privacy issues when considering new processing activities or setting up new procedures or systems that involve personal data. GDPR imposes a specify 'privacy by design' requirement, emphasising the need to implement appropriate technical and organisational measures during the design stages of a process and throughout the lifecycle of the relevant data processing to ensure that privacy and protection of data is not an after-thought.

For further information concerning techniques that can be used to reduce the risks associated with handling personal data, including 'Anonymisation and Pseudonymisation', see the Data Protection Guidance.

The University will assess what privacy by design measures can be implemented on all programs/systems/processes that process personal data by taking into account the following:

- the state of the art (i.e. the highest level of general development, as of a device, procedure, process or technique achieved at the particular time);
- the cost of implementation;
- the nature, scope, context and purposes of Processing; and
- the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

Data Protection Impact Assessments (DPIAs)
The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce risks.

For some projects, the GDPR requires that a Data Protection Impact Assessment (DPIA) is carried out. The types of circumstances when this is required include:

- those involving processing of large amounts of personal data, where there is automatic processing/profiling, processing of special categories of personal data, or monitoring of publicly assessable areas (i.e. CCTV).

The University will conduct DPIAs in respect of Processing which is considered to be high risk (for example where Processing involves Special Category Personal Data on a large scale).

The Data Protection Officer should be informed and a DPIA undertaken when implementing major system or business change programs involving the Processing of personal data including:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- automated Processing including profiling and automated decision making;
- large scale Processing of Special Category personal data; and
- large scale, systematic monitoring of a publicly accessible area (e.g. under CCTV).

Further information about when and how to carry out a DPIA can be found in the Data Protection Guidance.

Use of Third Party Data Processors
The University will ensure that all third party data processing is done under a written contract. This is to ensure that both parties understand its responsibilities and liabilities. Contract clauses will be used in line with those outlined under data protection law.

The University is liable for its compliance with data protection legislation and will only appoint processors who can provide 'sufficient guarantees' that the requirements of data protection law will be met and the rights of data subjects protected.

Automated Processing and Decision Making
In general terms, automated decision-making is prohibited when a decision has a legal or similar significant effect on an individual unless:

- an individual has explicitly consented;
- the processing is authorised by law; or
- the processing is necessary for the performance of or entering into a contract with the individual.

If certain types of Special Category Personal Data are being processed, then grounds (b) or (c) will not be allowed but such Special Category Personal Data can be processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on automated processing (including profiling), then Data Subjects must be informed in the Privacy Notice of the logic involved in the decision making or profiling, the significance and envisaged consequences. The Data Subject must also be and given the right to request human intervention, express their point of view or challenge (see guidance on Gathering Personal Data).

Data Subjects must also be informed that they have the right to object to this in the first communication with them (at the latest). This right must be explicitly brought to their attention and presented clearly and separately from other information.