1. **Introduction**

The University of Leicester is committed to protecting the privacy rights of individuals under data protection legislation and takes its responsibility for handling Personal Data very seriously. This policy sets out the fundamental requirements which are underpinned by sub-policies, procedures and more detailed guidance documentation.

 **2. Scope**

This policy applies to all Personal Data processed by the University for business and research purposes, irrespective of how that Personal Data is held. It therefore covers Personal Data held both electronically and on manual files/media and applies to all individuals who process Personal Data for, or on behalf of, the University.

The University of Leicester processes Personal Data of a wide range of individuals including (but not limited to) employees; honorary staff; research subjects; students; contractors and visitors.

The policy applies to all University employees; contractors; honorary staff and students who are processing Personal Data for which the University is a Data Controller. The Personal Data covered includes, but is not limited to data about employees; collaborators; students; alumni; visitors and research data subjects.

1. **Applicable laws**

This policy applies to Personal Data processed in accordance with the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR).

The policy gives due regard to Personal Data requirements under other law and regulations, including but not limited to:

Human Rights Act 1998

Privacy and Electronic Communications Regulations 2003

Regulation of Investigatory Powers Act 2000

Freedom of Information Act 2000

Environmental Information Regulations 2004

 Common Law Duty of Confidentiality

 Computer Misuse Act 1990

1. **Impact of Brexit & adequacy decision**

Following Brexit at the end of December 2020 the UK is now subject to the provisions of the UK GDPR which is tailored by the Data protection Act 2018. The UK GDPR is largely identical to the EU GDPR but there are some differences. Also, the UK GDPR mainly applies to controllers and processors located in the UK although there are some exceptions.

With reference to cross-border data flows from the EU to the UK, under the Trade and Cooperation Agreement between the UK and the EU, there were some provisions that allowed those transfers to continue on a temporary basis. This temporary arrangement came to an end on the 28th June 2021, when the EU approved adequacy decisions for the EU GDPR and the Law Enforcement Directive (LED). As a result, personal data can continue to flow between the UK and EU as it did before, in the majority of circumstances.

An EU adequacy decision means that a country, territory, sector or organisation are deemed to have an ‘essentially equivalent’ level of data protection to the EU. The adequacy decisions are in place for a period of 4 years, until 27th June 2025 at which point they will be reviewed by the European Commission.

An adequacy decision is not a permanent arrangement and can be reviewed by the European Commission at any point in time e.g. if it decides that the current UK data protection regime has changed to offer a lower level of protection.

1. **Data Protection Principles**

The Data Protection Principles are the foundation of data protection law. If properly adhered to, there is very little scope for breaching the applicable laws. All Personal Data must be processed in accordance with the seven Data Protection Principles below.

* **Lawfulness, fairness and transparency**

Personal shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

* **Purpose limitation**

Personal Data shall be 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 not be considered to be incompatible with the initial purposes.

* **Data minimisation**

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

* **Accuracy**

Personal Data shall be 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.

For example, University employees can update and change their own Personal Data through use of the Employee Self-Service. Students of the University can do the same through MyStudentRecord.

* **Storage limitation (retention)**

Personal Data shall be 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

* **Integrity and confidentiality (security)**

Personal Data shall be 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.

Technical measures include use of encryption, Firewall and Pseudonymisation. Organisational measures include policies and procedures, and data protection impact assessments (DPIAs).

* **Accountability**

The Data Controller shall be responsible for, and be able to demonstrate compliance with, the principles set out above. To meet the requirements of accountability the University as a Data Controller must have in place appropriate technical and organisational measures which include:

* Adopting and implementing **data protection policies**;
* Taking a **‘data protection by design and default’** approach (Refer to DPIA policy);
* Having **written contracts** in place with organisations that process Personal Data on the University’s behalf;
* **Maintaining documentation** **and a current record** of its processing activities;
* Implementing appropriate **security measures**;
* Recording and reporting internally and, where necessary, reporting **Personal Data breaches** to the ICO (Refer to data breach policy);
* Carrying out **data protection impact assessments** (DPIAs) for uses of Personal Data that are likely to result in high risk to individuals’ interests;
* Appointing a **data protection officer**; and
* Adhering to relevant **codes of conduct** and signing up to certification schemes.
1. **Records of processing activities (ROPA)**

The University is required to maintain a record of all processing activities under its responsibility. The record has to contain:

* **Name and contact details of the Controller (University) and where applicable details of the Joint Controller or the Controller’s representative.**
* **Name and contact details of the Data Protection Officer (see below)**
* **The purposes of the processing**
* **A description of the categories of data subjects and of the categories of Personal Data (what the Personal Data is)**
* **The categories of recipients to whom the Personal Data have been or will be disclosed including recipients in third countries or international organisations**
* **Where applicable, transfers of Personal Data to a third country or an international organisation. This should include details of that country or international organisation and where relevant documentation of suitable safeguards**
* **Where possible, the envisaged time limits for erasure of the different categories of data**
* **Where possible, a general description of the technical and organisational security measures in place**

As well as the above, the ROPA used by the University of Leicester also contains a number of questions to help undertake a preliminary risk assessment for a processing activity (a threshold DPIA). The records of processing activities at the University are stored within the OneTrust privacy management system.

It is the responsibility of process owners (whether researchers, academics or professional service staff) who manage or oversee data processing activities to ensure all activities in their control are accurately captured and reflected in the Records of Processing Activities and kept up to date according to the above requirements.

This is an organisational measure which falls under the obligations of the Accountability Principle and is a requirement of Article 30 of the UK GDPR. Please note that the ROPA entry needs completing when a new activity/initiative involving personal data is starting or a new process is being introduced and also when changing a process. In cases where a process changes, the original ROPA entry must be reviewed to ensure the changes are captured, this also enables risks to be identified at an early stage.

1. **Lawful basis for processing Personal Data**

At least one of the following lawful bases must apply when processing Personal Data. The single most appropriate basis should be selected.

**Consent**

The individual has given clear consent for the University to process their Personal Data for a specific purpose.

**Contract**

The processing is necessary for a contract the University has with the individual, or because they have asked the University to take specific steps before entering into a contract with them.

**Legal Obligation**

The processing is necessary for the University to comply with the law (not including contractual obligations covered separately).

**Vital Interests**

The processing is necessary to protect someone’s life.

**Public task**

The processing is necessary for the University to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law (e.g. equality and diversity reporting, HESA reporting).

**Legitimate interests**

The processing is necessary to meet the University’s legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual’s Personal Data, which overrides those legitimate interests. (This cannot apply if you are a public authority processing Personal Data to perform your official tasks.)

1. **Lawful basis for processing Special Category Data**

Listed below are the different types of Special Category Personal Data. This nature of data presents a higher risk to the rights and freedoms of individuals e.g. its processing in the wrong hands presents a higher risk of discrimination against an individual.

**Racial or ethnic origin Political opinions Religious or political beliefs Trade union membership Genetic data Biometric data**

**Health Sex life Sexual orientation**

Where Special Category data are processed an additional lawful basis to that for processing Personal Data, must be identified from those below.

1. **Explicit Consent**
2. **Employment, social security and social protection (if authorised by law)**
3. **Vital interests**
4. **Not-for-profit bodies**
5. **Made public by the data subject**
6. **Legal claims or judicial acts**
7. **Reasons of substantial public interest (with a basis in law)**
8. **Health or social care (with a basis in law)**
9. **Public health (with a basis in law)**
10. **Archiving, research and statistics (with a basis in law)**

If relying on conditions **b), h), i) or j)**, you also need to meet the associated condition set out in **Part 1 of Schedule 1 of the DPA 2018.** If you are relying on the substantial public interest condition in GDPR Article 9(2)(g), you also need to meet one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018. Contact Information Assurance Services (IAS) by emailing ias@leicester.ac.uk for further advice.

1. **Individual Rights**

Data Protection provides the following rights for individuals. Requests received by the University where individuals are exercising their rights are managed by IAS and require a response within **one calendar month**. There is no fee for exercising a right in most circumstances, in some cases, an exemption to the right may apply which means that sometimes the University will not need to provide the information, or part of the information, to the requestor. Some rights set out below are referred to as ‘not an absolute right’, which means that the University needs to give consideration to the application of an exemption.

* **The right to be informed**

Individuals have the right to be informed about the collection and use of their Personal Data at the time it is collected from them. This is usually through a Privacy Notice and there is a requirement to provide some specific information. See <https://le.ac.uk/policies/privacy>.

* **The Right of access**

Individuals can request to obtain a copy of the Personal Data held about them along with other supplementary information. This is known as a data subject access right (DSAR) and can be made verbally or in written form.

* **The right to rectification**

Individuals have the right to have inaccurate Personal Data rectified, or completed if it is incomplete.

* **The right to erasure – (‘right to be forgotten’)**

Individuals have the right to have Personal Data erased in certain circumstances. This is not an absolute right.

* **The right to restrict processing**

Individuals have the right to request a restriction or suppression of their Personal Data in certain circumstances. This is not an absolute right. Where it applies, the University is permitted to store the Personal Data but not use it.

* **The right to data portability**

This right allows individuals to obtain and reuse their Personal Data for their own purposes across different services. It allows them to move, copy or transfer Personal Data easily from one IT environment to another in a safe and secure way, without affecting its usability.

* **The right to object**

Individuals have the right to object to the processing of their Personal Data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing. However, in other cases where the right applies you may be able to continue processing if you can show you have a compelling reason for doing so.

* **Rights in relation to automated decision making and profiling**

Individuals have the right not to be subject to a decision based solelyon automated processing, including profiling, which produces legal effects on the individual or similarly significantly affects the individual.

Profiling means any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

It is important that information from central systems e.g. SITs and SAP **is not deleted locally**. Information from these systems is only deleted by IT Services in conjunction with IAS. For data held locally on sit alone systems a deletion request can be met by authorisation of the relevant manager in consultation with IAS.

1. **International Transfers**

Following the EU Commission’s adequacy decisions most personal data can continue to flow from the EU and the EEA without the need for any additional safeguards.

Under the UK regime restricted transfers from the UK to other countries (including EEA) are subject to transfer rules which are broadly similar to the EU GDPR rules. The key difference is that the UK has the independence to keep the framework under review and has transitional arrangements to help the transition to the new UK regime.

Provisions are in place to permit the transfer of personal data from the UK to the EEA and any countries which were covered by an EC adequacy decision on 31 December 2020. The UK government now has the power to make its own ‘adequacy decisions’, known as ‘adequacy regulations’, in relation to third countries and international organisations.

There are also provisions which allow the continued use of any EU Standard Contractual Clauses (SCC’s) which were valid on 31 December 2020. These apply to both existing restricted transfers and for new restricted transfers. There are also provisions that allow certain Binding Corporate Rules to transition into the UK regime.

**Restrictions on international transfers**

The UK GDPR restricts transfers of Personal Data to countries or to international organisations outside the UK or the protection of the UK GDPR, unless the rights of the individuals with regard to their Personal Data are protected or if an exception applies.

It is a restricted transfer if:

* The UK GDPR applies to the processing of the personal data you are transferring
* You are sending personal data, or making it accessible to a receiver to which the UK GDPR will not apply in relation to their processing of the personal data; and
* The receiver is legally distinct from you as it is a separate company, organisation or individual and includes transfers to another company within the same corporate group. It is important to note that if you are sending personal data to someone employed by you or by your company or organisation it is not a restricted transfer.

**How to make International Transfers in compliance with the UK GDPR**

Firstly, consider whether you can achieve your aim without sending personal data. If not, can you make the data anonymous which means an individual can never be identified from the information being transferred, even when that information is combined with other information available to the receiver. Anonymous data is not personal data and the restrictions would not apply.

Personal Data transfers can be made outside the UK by working through the following questions in order. If by the last question you are still unable to make the restricted transfer, then it will be in breach of the UK GDPR.

1. **Is the restricted transfer covered by Adequacy Regulations?**

A restricted transfer can be made where the receiver is located in a third country or territory or is an international organisation covered by UK adequacy regulations. These regulations set out in law that the legal framework where the receiver is located has been assessed as providing adequate protection for individuals’ rights and freedoms in relation to their Personal Data. This allows the restricted transfer to take place safely and legally without any additional measures being required.

Under provisional arrangements UK adequacy regulations include the EEA and all countries, territories and international organisations covered by EC adequacy decisions valid as at 31 December 2020.

Up to date information on adequacy regulations and decisions that have been made can be found at the following ICO website link [International Transfers](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/#adequacy).

1. **Is the restricted transfer covered by appropriate safeguards?**

Where there is no adequacy regulation for the country, territory or sector for a restricted transfer, it can still proceed subject to meeting appropriate safeguards listed in the UK GDPR. Each ensures that both you and the receiver of the restricted transfer are legally required to protect individuals’ rights and freedoms in respect of their personal data.

Before relying on an appropriate safeguard to make a restricted transfer, a **transfer impact assessment** to identify risk needs to be undertaken which takes into account the protections contained within that appropriate safeguard and the destination country (including laws governing public authority access to the data). This is to help ensure a level of protection equivalent to that under the UK data protection regime. If the assessment shows that the appropriate safeguard does not provide the required level of protection, then you can include additional measures.

The safeguards are set out below and more detail on the application of each can be found on the ICO’s website.

1. *A legally binding and enforceable instrument between public authorities or bodies*
2. *Binding corporate rules (BCRs)*
3. *Standard contractual clauses (SCCs)*
4. *An approved code of conduct*
5. *Certification under an approved certification scheme*
6. *Contractual clauses authorised by the ICO*
7. *Administrative arrangements between public authorities or bodies*
8. **Is the restricted transfer covered by an exception?**

Where the restricted transfer is not covered by UK ‘adequacy regulations’ or an appropriate safeguard, then you can only make that transfer if it is covered by one of the ‘exceptions’ set out in Article 49 of the UK GDPR. These are referred to as true ‘exceptions’ from the general rule **that you should not make a restricted transfer unless it is covered by UK ‘adequacy regulations’ or there are appropriate safeguards in place.**

The exceptions are set out below and more detail on the application of each can be found on the ICO’s website.

1. The individual has given explicit consent to the restricted transfer
2. You have a contract with the individual and the restricted transfer is necessary for you to perform that contract, or you are about to enter into a contract with the individual and the restricted transfer is necessary for you to take steps requested by the individual in order to enter into that contract.
3. You have (or are entering into) a contract with an individual which benefits another individual whose data is being transferred. The transfer is necessary for you to either enter into that contract or perform that contract.
4. You need to make the restricted transfer for important reasons of public interest.
5. You need to make the restricted transfer to establish if you have a legal claim, to make a legal claim or to defend a legal claim.
6. You need to make the restricted transfer to protect the vital interests of an individual. He or she must be physically or legally incapable of giving consent.
7. You are making a restricted transfer from a public register.
8. You are making a one-off restricted transfer and it is in your compelling legitimate interests.
9. **Training**

It is a legislative and University requirement that individuals subject to this policy must undertake an appropriate level of data protection and information security training reflective of the duties they are performing. Training is an organisational measure which falls under the obligations of the Accountability Principle. Training is mandatory and must be refreshed on an annual basis. Where appropriate the training will form part of the completion requirement of the University’s Personal Development Discussion (PDD) process. Evidence of equivalent training completed at a partner organisation approved by the Registrar e.g. University Hospitals Leicester (UHL), is also accepted. The majority of staff have to complete the University’s online training. Where this is not possible, additional off-line training is available to business areas through a request to IAS. Training may be exempted in very limited circumstances by the Registrar.

1. **Data Controller**

The University of Leicester is the Data Controller for the Personal Data that this policy applies to.

1. **ICO Registration No.**

The University is required to register with the Office of the Information Commissioner in relation to its data protection activities. The registration number can be obtained from Information Assurance Services (IAS) and is subject to change in April of each year.

1. **Data Protection Officer**

Parmjit Singh Gill

Data Protection Officer & Information Assurance Services Manager

T: 0116 252 7946

E: pg170@leicester.ac.uk

W: [www.le.ac.uk](https://eur03.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.le.ac.uk&data=02%7C01%7Cpg170%40leicester.ac.uk%7Cf907bdc14a264723158608d6d90b30d3%7Caebecd6a31d44b0195ce8274afe853d9%7C0%7C0%7C636935039419543265&sdata=jjBpiENYnG2gNiH4tvHuo2FOgS1pPepPwL1j4Hccv7Y%3D&reserved=0)

1. **Data Protection Enquiries**

At the University of Leicester enquiries relating to privacy rights and data protection matters are managed by Information Assurance Services, ias@le.ac.uk.

1. **Revision dates**

**Title:** Data Protection Policy

**Reference:** DPP

**Status:** Draft

**Version:** 3.0

**Date:** November 2021

**Date to Review:** August 2022

**Classification:** Open

**Author:** Parmjit Singh Gill

**Acknowledgement**

Extensive reference is made in this policy to text from the UK GDPR, Data Protection Act 2018 and guidance advice provided on the Information Commissioner’s website at [ico.org.uk](https://ico.org.uk).