Loughborough University Data Protection Policy

Section 1: Policy Scope

Loughborough University is committed to a policy of protecting the rights and privacy of individuals (includes students, staff and others) in accordance with the General Data Protection Regulation (2018) and Data Protection Act (2018). The University needs to process certain information about its staff, students and other individuals it has dealings with for operational purposes (e.g. to recruit and pay staff, to administer programmes of study, to record progress, to agree awards, to collect fees, to enable the effective delivery of its non-academic services to members of the University community, tenants and members of the public and to comply with legal obligations to funding bodies and government). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The policy applies to all staff and students of the University and the handling of all personal data processed by the University. Mandatory training is provided to staff to assist them in meeting their obligations under this policy. The University will investigate any breach of the General Data Protection Regulation (GDPR), Data Protection Act 2018 or the University Data Protection Policy. Where a personal data breach has occurred as a result of misconduct or malicious intent it is considered to be an offence and, in that event, Loughborough University disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with the University, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that Schools and services who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

Section 2: Data Protection Background

The purpose of the GDPR 2018 and Data Protection Act 2018 is to protect the rights and privacy of living individuals and to ensure that personal data and information is not processed without their knowledge, and, is processed with a clear legal basis. The University publishes information about the personal data it processes, and the legal basis for processing data, in its Data Privacy Notices (link). The University has an Information Categories and Controls policy (link) which provides guidance on the categorisation of the sensitivity and possible risks associated with different types of information and how each type may be shared and stored. Personal data and sensitive personal data ‘special category data’, as defined under the GDPR will normally fall into the Confidential Category in the policy.

Section 3: Information Governance Framework

Recognising that information is a vital asset, and that it is dependent upon strong information governance policies, processes, and practices; the University has established an Information Governance Framework. The framework and associated policies and procedures apply equally to all information and data throughout its entire lifecycle. It:

- Provides a structure in which the University's core data assets, within defined data domains, are managed in accordance with the overall University policy and framework; and
- Establishes clearly defined roles to coordinate and align the use of information held in, and across, each specific data domain (including personal identifiable information and data). The roles of 'Data Owner' and 'Data Steward' provide overall accountability for information in each data domain, as well as operational responsibility to implement information governance policy and procedures.

Section 4: Roles and Responsibilities

Loughborough University is registered with the Information Commissioner's Office as a Data Controller. Details of the University's registration are published on the Information Commissioner's website. The University as Data Controller shall implement appropriate technical and organisational measures to ensure that processing of personal information is performed in accordance with the GDPR (2018) and DPA (2018):

- The Data Protection Officer (The Chief Operations Officer), is responsible for ensuring that the University processes the personal information of its staff, students, customers, providers and partners in compliance with the applicable data protection rules,
- The University Information Governance Framework (See *Appendix 2: Information Governance Structure*) sets out clear roles of responsibility and accountability for managing personal information processed by the institution,
- Compliance with data protection legislation is the responsibility of all staff members and research students who process personal information. Guidance is available in the Responsibilities of Staff and Research Students and the Acceptable Use Policy (all staff and students),
- Members of the University (staff and students) are responsible for ensuring that any personal data they supply about themselves to the University are accurate and up to date. They are advised to familiarise themselves with the appropriate University privacy notice.

Section 5: GDPR Principles Relating to Processing of Personal Data

The University is accountable for, and will demonstrate it processes personal data in accordance with the six GDPR data protection principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

See Appendix 3 for detailed description of the GDPR principles relating to personal data.

Section 6: GDPR and Individual Rights

The University will observe and comply with the rights of the data subject, including the right to be informed (Data Privacy Notices) and the right of access (Subject Access Requests).

Data subject rights are not all ‘absolute rights’ and Loughborough University maintains the right to apply conditions or exceptions, where it has a lawful basis to do so. For example, where it has a legal obligation to retain or process personal data.

Section 7: Rights of Access to Data (Subject Access Requests)

- Individuals have the right to obtain confirmation from Loughborough University as to whether the University is processing personal data about them, and where that is the case, access to their personal data,
- Where the University is processing a large quantity of data concerning a data subject, it will request that, before the information is delivered, the individual specifies the information or processing activities to which the request relates,
- The University will check they have understood the requester’s access request if it is not clear,
- Any individual who wishes to exercise this right can request access either in writing or verbally. Requests can be made to any part of the University, although the University has a dedicated Subject Access Request service that can be contacted at dp@lboro.ac.uk,
- The requester must make it clear they are asking for their own information,
- The University will use all reasonable measures to verify the identity of a data subject who requests access. If it has any doubts about the identity of the person making the request it will ask for further information before responding to their request. In these instances, the request will only commence once the University has received additional information that verifies the requester’s identity,
- Any such requests will be complied with within one calendar month of receipt of the request,
- In exceptional circumstances to respond to a complex request, or a number of requests from a data subject, it may be necessary to extend the response date by up to a further two months. In these circumstances the University will inform the individual within one month of receiving their request; and
- In order to respond efficiently to subject access requests, the University needs to have in place appropriate records management practices.

Section 8: Lawful Basis for Processing Personal Data

The GDPR provides six lawful bases for processing personal data. The University will only process personal data where it is necessary and it has identified at least one valid lawful basis, decisions on the appropriate lawful basis will be based on the specific purpose and context of the processing.

Lawful Basis	Justification for Processing
Public Task	Necessary to perform a task in the public interest or for an official function.
Contract	Necessary for fulfilling a contract or to enter into a contract.
Legal Obligation	Necessary to comply with the law (excluding contracts).
Vital Interest	Necessary to protect the life of the individual, or another individual.
Legitimate interest	Necessary for the University's legitimate interests or the legitimate interest of another party, unless it would undermine the interests of an individuals' right to privacy.
Consent	Consent must be freely given, specific, informed and unambiguous. The data subject must be informed of their absolute right to withdraw consent at any time.

Before processing of personal data begins, staff are responsible for ensuring that:

- There is no other way to reasonably achieve the same outcome, without processing personal data,
- Valid lawful bases and justifications for processing personal data have been identified and documented. There may be more than one lawful basis, in which case they should all be identified and recorded,
- Information about the lawful basis and intended purpose for processing information is included in the privacy notice; and
- In instances where sensitive personal (special category) data, criminal convictions data, or data about offences will be processed; the University will have identified an additional condition for processing, as described in Article 9 GDPR: processing of special categories of personal data. For example, it has obtained the explicit consent of the individual, it is necessary to protect the vital interest of an individual/s, the information had already been made public by the individual, or it necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Other conditions for processing special category information exist and can be found in Article 9 GDPR.

If any member of the University is in any doubt about these matters, they should consult the relevant Data Steward (as set out in the University Information Governance Framework) or their local Data Co-Ordinator.

Section 9: Sharing/Disclosing Personal Information

The University may legitimately share personal information either within the University, or with an external third party, provided it has identified at least one valid lawful basis (See *Section 8: Lawful Basis for Processing Personal Data*). In cases where it is necessary to share sensitive personal (special category), extra care must be taken. The GDPR (2018) imposes additional limits on the circumstances in which special category information can be shared, the kinds of information this applies to includes: racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, genetics data, biometric data (to identify individuals), data concerning health (including mental health and conditions), sex life, and sexual orientation. Additional information can be found in section 8 of this policy.

The University will publish in the relevant privacy notice, instances where it is necessary to disclose personal information to other parties to complete a task.

The University will ensure that personal data is processed in a secure way, including protection against unauthorised or unlawful disclosure (sharing); including sharing information with third parties which includes family members, friends, government bodies, and in certain circumstances, the Police.

In some exceptional circumstances The Data Protection Act (2018) permits certain disclosures as exemptions from GDPR:

- to safeguard national security,
- the maintenance of effective immigration control,
- prevention or detection of crime including the apprehension or prosecution of offenders,
- assessment or collection of tax or duty; and
- discharge of regulatory functions (includes health, safety and welfare of persons at work).

These exemptions should not be routinely relied upon, each disclosure needs to be considered on a case-by-case basis and requests must be supported by suitable documentation recording the reason for the decision.

University staff and student may not disclose any data about data subjects (e.g. employees, students, applicants or research participants), including information as to whether a named individual is, or has been a member of the University unless they are clear they have the authority of either the University, or the named individual to do so.

When sharing personal information, staff and students should refer to the University's Information Sharing Policy.

If in doubt, staff should seek advice from their Data Co-Ordinator in the first instance or consult with the appropriate Data Steward.

Section 10: Data Protection by Design and Default (Data Privacy Impact Assessment)

Loughborough University is committed to ensuring privacy is built into its services, processes and systems. Where it is processing personal data, the University will apply the concept of 'data protection by design and default'. This means that data protection is considered from the outset and is integrated into the University's activity from the design stage and right through the data lifecycle to safeguard individuals' right to privacy.

The effective deployment of the University's corporate systems will play a key role in the secure management of personal data held by the University. To this end, the University has introduced two new roles as part of an information governance, university structure; that of Data Owner and Data Steward (see Appendices). They will play an active role in ensuring the University is accountable for protecting individual's privacy in the University's core data domains; and provide operational responsibility for data protection compliance for specific information assets.

Where the University proposes using personal data derived from its core data domains to improve the quality or efficacy of its services, the Data Stewards will provide the first point of liaison where data issues are identified.

Where processing personal data is likely to result in a high-risk to individual's privacy, new projects or systems (including Software as a Service) must conduct a Data Privacy Impact Assessment (DPIA) to identify potential risk and determine measures to minimise those risks. The DPIA must be signed off by the Data Steward(s) for the relevant Data Domain(s).

Section 11: Security of Data

All staff are responsible for ensuring that personal data they process is kept secure and managed in accordance with the Information Categories and Controls Policy, that it is not disclosed to any unauthorised third party (see *Section 9: Sharing/Disclosing Personal Information* for more detail).

Personal data shall only be accessible to those who need to use it, it should be stored in secure, password protected and corporate approved information systems (or locked cabinets if in hardcopy). Care must be taken to ensure that appropriate security measures are in place for access to personal data and information. The University's policy on the Management of User Access to Information provides guidance in this area. This policy also applies to staff and students who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and students should take particular care when processing personal data away from their desk (whether on or off campus) and guidance will be found in the University's Mobile Working Policy.

Section 12: Personal Data Breach

In the event of a personal data breach, unless it is unlikely to result in a risk to the rights and freedoms of an individual/s, the University must notify the Information Commissioner's Office (ICO) of the incident, no later than 72 hours of first becoming aware of the problem. Risk to the rights and freedoms of an individual is not limited to, but might include risk of identity theft or fraud, damage to reputation, loss of control over personal data, or risk of discrimination.

If the personal data breach is likely to result in a high risk to an individual/s, they should also be notified, without unreasonable delay and told the nature of the event as well as recommendations for how they might take remedial action

If a member of staff or student suspects or discovers a personal data breach, including unauthorised or unlawful processing, accidental loss, destruction or damage to personal data they must report it immediately using the 'Report a data breach' guidance available on the University webpages. Staff should also report a breach to their nominated Data Coordinator without delay.

Section 13: Retention and Disposal of Data

The University will not keep personal data for longer than is necessary for the purpose it was being processed for. Staff are responsible for complying with the retention period for different categories of information, ultimately the Data Owner is accountable for ensuring that personal data that has reached the end of its retention period is either destroyed or anonymised. Data which has been anonymised so that all identifying information has been removed, may be kept indefinitely.

There may be some instances where the University will retain personal information for longer to fulfil some specific purposes: archiving (where it is in the public interest), specific historical or scientific research, or statistical purposes. As this processing is subject to stricter conditions of use, safeguards must be put in place to protect the rights of data subjects.

Where individuals make a request for their personal information to be deleted, the University will review its retention schedule to identify if there are any possible reasons why it might not be able to comply with the request, e.g. where it has a statutory, regulatory, legal or a security reason to retain information.

Academic Schools and Professional Services are responsible for regularly reviewing any locally held personal information, in accordance with the University retention schedule.

Disposal of Records

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion). It must be securely destroyed in accordance with University security policy. Processes must be in place to ensure that all backups and copies are included in the destruction of data, and to see that any personal data pending audit, litigation, investigation, or being processed as part of an outstanding subject access request are not destroyed.

Section 14: Publication of University Information

All members of the University should note that the University publishes a number of items that include personal data, applying a lawful basis of legitimate interest, engagement in a public task, or consent. These personal data are:

- Names of all members of University Committees (including Council and Senate),
- Names, job titles and academic and/or professional qualifications of members of staff,
- Awards and Honours (including Honorary Graduands and Prize winners)
- Internal Telephone Directory,
- Graduation programmes and videos or other multimedia versions of graduation ceremonies,
- Information in prospectuses (including photographs), annual reports, staff newsletters, etc. and
- Staff information on the University website (including photographs).

It is recognised that there might be occasions when a member of staff, a student, or a lay member of the University, requests their right to either restrict processing or erase their personal details. These are not absolute rights, meaning the University will need to consider if the information is needed for another valid reason, for example, to comply with a legal obligation or for archiving purposes in the public interest.

Section 15: Direct Marketing

Direct marketing is defined by the ICO as ‘the promotion of aims and ideas as well as the sale of products and services’ which are directed to particular individuals.

In most circumstances, Schools or Services must only send marketing information to people who have specifically said they agree to LU doing this. For consent to be lawful, it must be freely given, specific, and informed. The request must be distinct and presented using clear and plain language. The University must also demonstrate that individuals have provided their consent, so records of consent must be kept for as long as their data is needed.

University employees must not contact individuals to ask them to re-consent to their information being used for the purpose of direct marketing; it might be necessary from time to time to contact individuals to provide an opportunity for them to update their details.

Individuals have the right to opt-out of receiving information they have previously consented to receive. Every direct marketing email communication should include an option to opt-out or unsubscribe from receiving future information. Where an individual decides to opt-out of receiving further communications, their request should be acted upon within 30 days.

In exceptional circumstances, it may be possible to use legitimate interest as the legal basis for direct marketing by electronic means if there is a clear benefit to the institution, the privacy impact on the individual is limited, and the benefit to the University doesn’t outweigh the impact on the person. For example, most processing of business contact data will be lawful based on legitimate interest as data about people in their professional capacity is regarded as less sensitive.

For legitimate interest to be a lawful basis for direct marketing, the Service/School must conduct and record their findings from a three-part legitimate interest test (the purpose

test, the necessity test and the balancing test). It is essential to consider the nuisance factor of unwanted or overly frequent marketing messages. Every communication should include an option to opt-out or unsubscribe from receiving further communications.

Section 16: Use of CCTV

The University's use of CCTV is regulated by a separate policy (Loughborough University CCTV Policy), designed to ensure that the Close Circuit Television (CCTV) system used at Loughborough University is operated in compliance with the law relating to data protection, and includes the principles governing the processing of personal data.

Section 17: Academic Research

Personal data collected only for the purposes of academic research (includes work of staff and students) must be processed in compliance with The GDPR and the Data Protection Act 2018. For further guidance on the collection and use of personal data for research purposes see the Additional Information on the Ethical Approval (Human Participants) Sub-Committee website.

Researchers should ensure that the results of the research are anonymised when published and that no information is published that would allow individuals to be identified.

Date of approval: 21 November 2019

Date of link updates: 9 January 2023

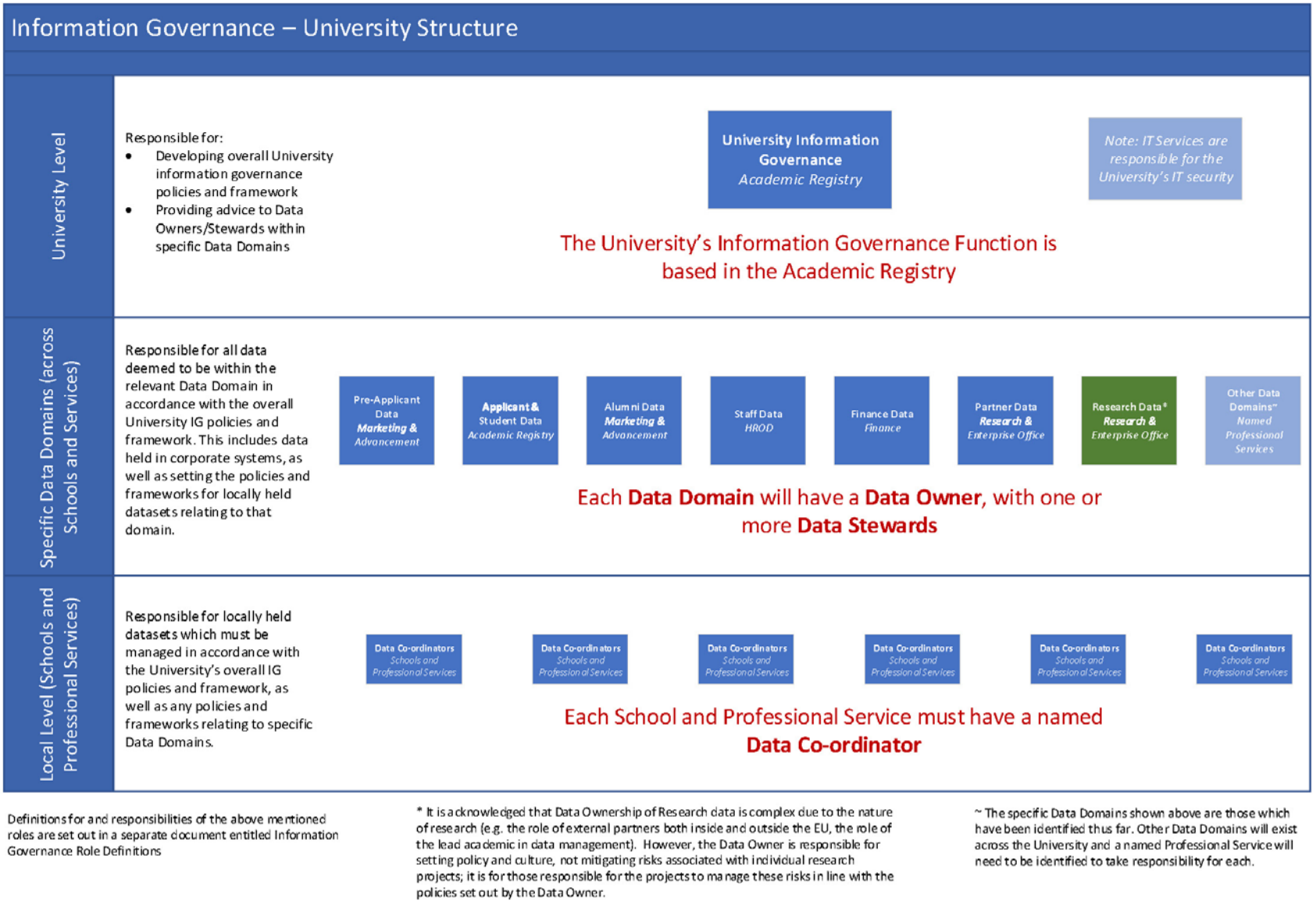
Document Owner: Academic Registry

Appendices

Appendix 1: Definitions (GDPR (2018) Definitions)

Personal Data	Any information or data relating to an identified or identifiable living individual who can be identified, directly or indirectly, in particular by reference to a name, and identification number, location data, an online identifier or to one of more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
Sensitive Data/ Special Category Data	Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, sexual orientation, criminal convictions, genetic data and biometric data. Special category data are subject to much stricter conditions of processing.
Data Subject	Any living individual who is the subject of personal data held by an organisation.
Data Controller	Any person (or organisation) which alone or jointly with others, determines the purpose and means of processing of personal data.
Data Processor	Any person or organisation which processes personal data on behalf of the Data Controller.
Third Party	Any individual/organisation other than the data subject, the data controller, or data processor who, under the direct authority of the controller or processor, are authorised to process personal data.
Processing	Any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Lawful Basis	Processing personal data will only be legal if it is necessary, and a lawful basis for processing has been identified. These lawful basis could be for a contract, to comply with a legal obligation, to protect the vital interests of a person, a task carried out in the public interest, a legitimate interest (except where it exceed the privacy interests of a data subject), or the data subject has given their explicit consent to process their personal information.
Relevant Filing System	Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. Personal data can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

Appendix 2: Information Governance Framework



Definitions for and responsibilities of the above mentioned roles are set out in a separate document entitled Information Governance Role Definitions

* It is acknowledged that Data Ownership of Research data is complex due to the nature of research (e.g. the role of external partners both inside and outside the EU, the role of the lead academic in data management). However, the Data Owner is responsible for setting policy and culture, not mitigating risks associated with individual research projects; it is for those responsible for the projects to manage these risks in line with the policies set out by the Data Owner.

~ The specific Data Domains shown above are those which have been identified thus far. Other Data Domains will exist across the University and a named Professional Service will need to be identified to take responsibility for each.

Appendix 3: Principles of GDPR

GDPR Principles relating to processing of personal data

All processing of personal data and information must be done in accordance with the six data protection principles set out in the GDPR (2018). 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**); and
- 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 4: GDPR and Individual Rights

The GDPR provides the following eight rights for individuals, individuals have:

1. The right to be informed

   They have the right to know, what personal information about them is being collected, how it is being used, how long it will be kept for and whether it will be shared with any other parties,

2. The right of access

   They may submit subject access requests (request for personal information the University holds on them), Loughborough University must provide a copy of any personal data it holds within one calendar month of making the request,

3. The right of rectification

   If an individual finds that the personal information Loughborough University holds on them is inaccurate or incomplete, they can request that it is updated within one month of making the request,

4. The right to erasure

   An individual can request that Loughborough University erases their personal data. For example, when it is no longer necessary for the University to keep it or they have withdrawn their consent for the University to process their personal data.

5. The right to restrict processing:

   An individual can request that the University limits the way it uses their personal data. For example, in cases where they wish to contest the accuracy of the personal data the University holds about them.

6. The right to data portability

   They have the right to obtain and reuse; or have their personal data the University holds on them transmitted in a structured, commonly used and machine-readable format to another data controller, to take advantage of other services.

7. The right to object:

   Individuals have the right to object to the processing of their personal data. They might disagree with decisions the University has made about its lawful basis for processing their personal data e.g. legitimate interest.

8. Rights related to automated decision making / profiling

   They have the right to request human intervention, or to challenge a decision made using an automated individual decision-making process (including profiling).

Appendix 5: Policy on processing of special categories of personal data and criminal offence data

As part of Loughborough University's statutory and corporate functions, it processes special category data and criminal offence data in accordance with Article 9 and 10 of the GDPR and Schedule 1 of the Data Protection Act 2018 (DPA).

Schedule 1 of the DPA requires the University to put in place an appropriate policy document, setting out our procedures for complying with article 5 of the GDPR, how long it will keep special category data for, and its subsequent erasure once it reaches its retention data.

This document explains our processing and satisfies the requirements of Schedule 1, part 4 of the DPA and supplements the University's staff and student privacy notices. It satisfies the substantial public interest condition, plus the condition for processing employment, social security, and social protection data where an appropriate policy document is required.

Special category data

Article 9 of the GDPR defines special category data as personal data revealing a person's:

- Racial or ethnic origin,
- Religious or philosophical beliefs,
- Political opinions,
- Trade union membership,
- 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

Criminal Conviction data

Article 10 of the GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

Conditions for processing special category data

GDPR

We process special categories of personal data under the following GDPR Articles:

Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on Loughborough University or the data subject in connection with employment, social security or social protection. For example, staff sickness absence.

Article 9(2)(g) - reasons of substantial public interest. Our processing of personal data in this context is for the purposes of substantial public interest and is necessary for the carrying out of our role. For example, monitoring equality of opportunity or treatment between groups

Article 9(2)(f) – for the establishment, exercise or defence of legal claims. For example, processing relating to any employment tribunal or other litigation.

Article 9(2)(a) – explicit consent

In circumstances where we seek consent, it is unambiguous and for specified purpose(s), it is given by an affirmative action, and recorded as the condition for processing. For example, staff or student reasonable adjustments.

Article 9(2)(c) – where processing is necessary to protect the vital interests of the data subject or of another natural person. For example, processing health data in the event of a medical emergency.

We process **criminal offence data** under Article 10 of the GDPR. For example, for pre-employment or pre-registration checks and declarations by an employee/student in line with contractual obligations.

DPA 2018

We process special categories of personal data for the following purposes in Part 1 of Schedule 1:

Paragraph 1(1) employment, social security and social protection

We process special category data for the following purpose in Part 2 of Schedule 1:

Paragraph 6(1) and (2)(a) statutory, etc. purposes
Paragraph 8(1) identifying or keeping under review the existence or absence of equality of opportunity or treatment between specified groups.
Paragraph 10(1) preventing or detecting unlawful acts
Paragraph 11(1) and (2) protecting the public against dishonesty
Paragraph 12(1) and (2) regulatory requirements relating to unlawful acts and dishonesty
Paragraph 24(1) and (2) disclosure to elected representatives

In **Paragraph 8(1)** the University must stop processing personal data if the data subject(s) has given notice in writing, requiring the university to stop processing their personal data, the notice gave the University a reasonable period in which to stop processing the data, and that period has ended.

Criminal offence data

We process criminal offence data for the following purposes in parts 1 and 2 of the DPA, Schedule 1:
Paragraph 1 employment, social security and social protection
Paragraph 6(2)(a) statutory, etc. purposes

Description of data processed

We process special category data about our staff and students that is necessary to fulfil our obligations as a higher education provider and employer, including information about, health and wellbeing, race and ethnicity, and trade union membership. Further information can be found in the University's staff and student privacy notices.

We also keep and maintain a record of our processing activities in accordance with article 30 of the GDPR.

Procedures for ensuring compliance with the GDPR principles

The University has put in place appropriate technical and organisational measures (policies, procedures, and processes) to meet the obligations set out in the GDPR and DPA. These include, but are not limited to, the following:

- The appointment of a data protection officer who reports into the university's highest management level;
- An information governance framework built on the principle of 'data protection by design and default;
- Carrying out data protection impact assessments for high risk personal data processing;
- Clear and transparent information about processing personal data in the university's privacy notices; and
- Electronic information is processed within the university's secure network, using systems that have appropriate security and access controls applied.

Retention and erasure policies

Our retention and erasure practices are set out in the University retention schedules here.

Appropriate Policy Document

This policy will be retained for the duration of out processing and for a minimum of 6 months after processing ceases.

This policy will be reviewed every two years or revised more frequently if necessary.