Privacy and Personal Data Protection Policy

1 Scope and Purpose

In its everyday business operations Loughborough College makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective employees
- Current, past and prospective students
- Customers
- Users of its websites
- Subscribers
- Other stakeholders

In collecting and using this data, the organisation is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps Loughborough College is taking to ensure that it complies with it.

This control applies to all systems, people and processes that constitute the organisation’s information systems, including board members, directors, employees, suppliers and other third parties who have access to Loughborough College systems.

The following policies and procedures are relevant to this document:

- Data Protection Impact Assessment Process
- Personal Data Mapping Procedure
- Information Security Incident Response Procedure
- Roles, Responsibilities and Authorities
- Records Retention and Protection Policy

2 Privacy and Personal Data Protection Policy

2.1 Data Protection Legislations & Regulations

The UK’s Data Protection Act 2018, the UK GDPR and the EU’s General Data Protection Regulation (GDPR) some of the most significant pieces of legislation affecting the way that Loughborough College carries out its information processing activities. These laws are designed to protect the personal data of all citizens whilst their data is being processed within UK, EEA, and also citizens data being processed anywhere in the world. It is Loughborough College’s policy to ensure that our compliance with these laws and other relevant legislation is clear and demonstrable at all times.
2.2 Definitions

The most fundamental definitions with respect to this policy are as follows:

**Personal data** is defined as:

any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

‘processing’ means:

any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

‘controller’ means:

the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

‘processor’ means:

the natural or legal person or organisation that acts on behalf of the controller, processing data only based upon written instructions only with no deviation unless authorised by the controller. They must equally ensure confidentiality and compliance, and inform the controller of any infringements. They keep records of all processing activities carried out on behalf of the controller.

2.3 Principles Relating to Processing of Personal Data

There are a number of fundamental principles upon which the legislations are based.

These are as follows:

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

(b) 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’);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(d) 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’);

(e) 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’);

(f) 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’).

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

Loughborough College must ensure that it complies with all of these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems.

2.4 Rights of the Individual

The data subject also has rights under both laws. These consist of:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.
Each of these rights will be supported by appropriate procedures within Loughborough College that allow the required action to be taken within the timescales stated in the legislations.

These timescales are shown in Table 1.

<table>
<thead>
<tr>
<th>Data Subject Request</th>
<th>Timescale</th>
</tr>
</thead>
<tbody>
<tr>
<td>The right to be informed</td>
<td>When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)*</td>
</tr>
<tr>
<td>The right of access</td>
<td>One month*</td>
</tr>
<tr>
<td>The right to rectification</td>
<td>One month*</td>
</tr>
<tr>
<td>The right to erasure</td>
<td>Without undue delay*</td>
</tr>
<tr>
<td>The right to restrict processing</td>
<td>Without undue delay*</td>
</tr>
<tr>
<td>The right to data portability</td>
<td>One month*</td>
</tr>
<tr>
<td>The right to object</td>
<td>On receipt of objection*</td>
</tr>
<tr>
<td>Rights in relation to automated decision making and profiling.</td>
<td>Not specified*</td>
</tr>
</tbody>
</table>

*Timescale as per table 1 – Unless not possible where appropriate reasons will be given for not complying

Table 1 - Timescales for data subject requests

2.5 Lawfulness of Processing

There are six ways in which the legitimacy of processing personal data may be established. It is Loughborough College’s policy to identify the appropriate basis for processing and to document it, in accordance with the Regulation. The options are described in brief in the following sections.

2.5.1 Consent

Unless it is necessary for a reason allowable, Loughborough College will always obtain explicit consent from a data subject to collect and process their data. In case of children below the age of 16 (a lower age may be allowable in specific EU member states) parental consent will be obtained. Transparent information about our usage of their personal data will be provided to data subjects at the time that consent is obtained and their rights with regard to their data explained, such as the right to withdraw consent. This information will be provided in an accessible form, written in clear language and free of charge.

If the personal data is not obtained directly from the data subject then this information will only be processed if in connection with a data subject in relation to the education, training or employment (or prospective/past education, training or employment) at Loughborough College.

2.5.2 Contractual Necessity

Where the personal data collected and processed are required to fulfil a contract with the data subject, explicit consent is not required. This will often be the case where the contract cannot be completed without the personal data in question e.g. a delivery cannot be made without an address to deliver to.
2.5.3 Legal Obligation
If the personal data is required to be collected and processed in order to comply with the law, then explicit consent is not required. This may be the case for some data related to employment and taxation for example, and for many areas addressed by the public sector.

2.5.4 Vital Interests
In a case where the personal data is required to protect the best interests of the data subject or of another natural person, then this may be used as the legitimate basis of the processing. Loughborough College will retain reasonable, documented evidence that this is the case, whenever this reason is used as the legitimate basis of the processing of personal data. As an example, this may be used in aspects of social care, particularly in the public sector.

2.5.5 Public Interest
Where Loughborough College needs to perform a task that it believes is in the public interest or as part of an official duty then the data subject’s consent will not be requested. The assessment of the public interest or official duty will be documented and made available as evidence where required.

2.5.6 Legitimate Interests
If the processing of specific personal data is in the legitimate interests of Loughborough College and is judged not to affect the rights and freedoms of the data subject in a significant way, then this may be defined as the lawful reason for the processing. Again, the reasoning behind this view will be clearly identified.

2.6 Privacy by Design
Loughborough College has adopted the principle of privacy by design and will ensure that the definition and planning of all new or changed systems that collect or process personal data will be subject to due consideration of privacy issues. Where there is a high risk to the data subject there will be the completion of a data protection impact assessment.

The data protection impact assessment will include

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimization, pseudonymisation and anonymisation should be considered where applicable and appropriate.
2.7 Contracts involving the Processing of Personal Data

Loughborough College will ensure that all relationships it enters into that involve the processing of personal data are subject to a documented contract that includes the specific information and terms required.

2.8 International Transfers of Personal Data

Transfers of personal data outside the European Union must be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the legislations. This depends partly on the European Commission’s judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.

Intra-group international data transfers must be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

2.9 Data Protection Officer

A defined role of Data Protection Officer (DPO) is required if an organization is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

Based on these criteria, Loughborough College requires a Data Protection Officer to be appointed.

2.10 Breach Notification

It is Loughborough College’s policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the legislation, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant Data Protection Authority (DPA) will be informed within 72 hours. This will be managed in accordance with our Information Security Incident Response Procedure, which sets out the overall process of handling information security incidents.

2.11 Addressing Compliance

The following actions will be undertaken to ensure that Loughborough College complies at all times with the accountability principle of the DPA2018, UK GDPR & EU GDPR:

- The legitimate basis for processing personal data is clear and unambiguous
- A Data Protection Officer is appointed with specific responsibility for data protection in the organisation
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff
- Rules regarding consent are followed
• Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively
• Regular reviews of procedures involving personal data are carried out
• Privacy by design is adopted for all new or reviewed systems and processes
• The following documentation of processing activities is recorded:
  o Organisation name and relevant details
  o Purposes of the personal data processing
  o Categories of individuals and personal data processed
  o Categories of personal data recipients
  o Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place
  o Personal data retention schedules
  o Relevant technical and organisational controls in place

These actions will be reviewed on a regular basis as part of the management review process of the data protection management system.

3 Equality Impact Assessment

This policy/procedure has been assessed for its impact on equal opportunities and will be informed by the aim to eliminate all forms of discrimination in all strands of the equal opportunities legislation – can only be inserted once EIA is received from E&D Manager

4 Location and Access to the Policy
SharePoint

5 Persons Responsible for the Policy
Data Protection Officer
CEO

6 Linked Policies and Procedures
• Data Protection Impact Assessment Process
• Personal Data Mapping Procedure
• Information Security Incident Response Procedure
• Roles, Responsibilities and Authorities
• Records Retention and Protection Policy

7 Change log

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Details of change</th>
<th>Review / Revision by</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Page 7 of 8</td>
<td>Document Ref: <strong>DP-P001</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Version 1.4</td>
<td>Last review: Sep 2023</td>
</tr>
<tr>
<td>Applicable to: All staff</td>
<td>Approved by: VP People and Planning</td>
<td>Accessible to: All staff</td>
<td></td>
</tr>
</tbody>
</table>

This document is the property of Loughborough College.
Any reproduction, even partial, is prohibited without prior written agreement.
Document uncontrolled when printed.
<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description</th>
<th>Revised by</th>
<th>Approved by</th>
</tr>
</thead>
<tbody>
<tr>
<td>19/02/18</td>
<td>1.1</td>
<td>Updated section 2.5 Added section 2.7 and renumbered following sections</td>
<td>Colin Butler</td>
<td>VP People and Planning</td>
</tr>
<tr>
<td>21/02/20</td>
<td>1.2</td>
<td>Review of Document. Couple of additions and minor amendments</td>
<td>James Kilby-Brooks</td>
<td>Data Protection Advisor</td>
</tr>
<tr>
<td>18/05/21</td>
<td>1.3</td>
<td>General review and tweak to a few terms following Brexit</td>
<td>James Kilby-Brooks</td>
<td>Data Protection Advisor</td>
</tr>
<tr>
<td>28/03/23</td>
<td>1.4</td>
<td>Tweak to a few of the terms to focus on wider data protection rather than GDPR</td>
<td>James Kilby-Brooks</td>
<td>Data Protection Advisor</td>
</tr>
</tbody>
</table>