**Data Protection Policy**

## Section 1: Policy Statement

TrainerMaker is committed to a policy of protecting the rights and privacy of individuals (includes students, staff and others) in accordance with the Data Protection Act. Trainermaker needs to process certain information about its staff, students and other individuals it has dealings with for operational purposes (eg to recruit and pay staff, to administer programmes of study, to record progress, to agree awards, to collect fees, 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 TrainerMaker. Mandatory training is provided to staff to assist them in meeting their obligations under this policy. Any breach of the Data Protection Act 1998 or the TrainerMaker Data Protection Policy is considered to be an offence and in that event, TrainerMaker disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with TrainerMaker, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that partners to TrainerMaker will sign a contract agreeing to abide by this policy.

## Section 2: Background

The purpose of the Data Protection Act 1998 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, wherever possible, is processed with their consent. Personal data and sensitive personal data as defined under the Act will normally fall into the Confidential Category in the policy.

**Section 3: Definitions (Data Protection Act 1998)**

|  |  |
| --- | --- |
| **Personal Data** | Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, telephone number, id number. Also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual. |
| **Sensitive 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, criminal convictions. Sensitive data are subject to much stricter conditions of processing. |
| **Data Controller** | Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed. |
| **Data Subject** | Any living individual who is the subject of personal data held by an organisation. |
| **Processing** | Any operation related to organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data Accessing, altering, adding to, merging, deleting data Retrieval, consultation or use of data Disclosure or otherwise making available of data. |
| **Third Party** | Any individual/organisation other than the data subject, the data controller (University) or its agents. |
| **Relevant Filing System** | Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. **Please note that this is the definition of "Relevant Filing System" in the Act. Personal data as defined, and covered, by the Act 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.** |

## 

## Section 4: Responsibilities under the Data Protection Act

* TrainerMaker is the data controller under the Act.
* A Data Protection Officer has been appointed who is responsible for day-to-day data protection matters and for developing specific guidance notes on data protection issues for employees and students of TrainerMaker
* Students and staff are responsible for ensuring that any personal data they supply about themselves to TrainerMaker are accurate and up-to-date.

## Section 5: Registration as a Data Controller

TrainerMaker is required to register with the Information Commissioner’s Office as a Data Controller. Details of the TrainerMaker's registration will be published on the [Information Commissioner's website](https://ico.org.uk/ESDWebPages/Entry/Z3179802).

## Section 6: Data Protection Principles

All processing of personal data and information must be done in accordance with the nine data protection principles.

1. **Personal data shall be processed fairly and lawfully.**  
   Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.
2. **Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.**Data obtained for specified purposes must not be used for a purpose that differs from those.
3. **Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.**Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data are given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.
4. **Personal data shall be accurate and, where necessary, kept up to date.**Data, which are kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that data held by the University are accurate and up-to-date. Completion of an appropriate registration or application process will be taken as an indication that the data contained therein is accurate. Individuals should notify the University of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the University to ensure that any notification regarding change of circumstances is noted and acted upon.
5. **Personal data shall be kept only for as long as necessary.** (see Section 12 on [Retention and Disposal of Data](https://www.lboro.ac.uk/admin/ar/policy/dpact/ludpp/#sec12))
6. **Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.**(see Section 7 on [Data Subjects Rights](https://www.lboro.ac.uk/admin/ar/policy/dpact/ludpp/#sec7))
7. **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.**(see Section 9 on [Security of Data](https://www.lboro.ac.uk/admin/ar/policy/dpact/ludpp/#sec9))
8. **Personal data shall not be transferred to a country or a territory outside the European Economic Area 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.**
9. Data must not be transferred outside of the European Economic Area (EEA) - the twenty-eight EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual. Secure methods for sharing information will be found in the [Information Sharing Policy](http://www.lboro.ac.uk/services/registry/information-governance/policy7/).

## Section 7: Data Subject Rights

Data Subjects have the following rights regarding data processing, and the data that are recorded about them:

* To make subject access requests regarding the nature of information held and to whom it has been disclosed.
* To prevent processing likely to cause damage or distress.
* To prevent processing for purposes of direct marketing.
* To be informed about mechanics of automated decision taking process that will significantly affect them.
* Not to have significant decisions that will affect them taken solely by automated process.
* To sue for compensation if they suffer damage by any contravention of the Act.
* To take action to rectify, block, erase or destroy inaccurate data.
* To request the Commissioner to assess whether any provision of the Act has been contravened.

## Section 8: Consent

Wherever possible, personal data or sensitive personal data should not be obtained, held, used or disclosed unless the individual has given consent. TrainerMaker understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as consent given as part of completion of an on-line form, physical signing a form or in email format and a record of the consent should be retained. The individual must give consent freely and of their own accord. Consent cannot be inferred from non-response to a communication. For sensitive personal data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances consent to process personal and sensitive data is obtained routinely by the TrainerMaker (eg when a student completes the registration process or when a new member of staff accepts a contract of employment). Any TrainerMaker forms (whether electronic or paper-based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. If an individual does not consent to certain types of processing (eg direct marketing), appropriate action must be taken to ensure that the processing does not take place.

If any student or employee of TrainerMaker is in any doubt about these matters, they should consult the TrainerMaker Data Protection Officer.

## Section 9: Security of Data

All staff are responsible for ensuring that any personal data (on others) which they hold are kept securely and in accordance with the Data Protection Policy and that they are not disclosed to any unauthorised third party (see Section 11 on [Disclosure of Data](http://www.lboro.ac.uk/admin/ar/policy/dpact/ludpp/index.htm#sec11) for more detail).

All personal data should be accessible only to those who need to use it. Such data and information should be stored in secure, password protected and normally corporate information systems (or locked locations 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 10: Rights of Access to Data (Subject Access Requests)

TrainerMaker employees or students have the right to access any personal data about themselves which are held by the TrainerMaker in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by the TrainerMaker about that person.

Any individual who wishes to exercise this right should apply in writing to the Data Protection Officer. TrainerMaker reserves the right to charge a fee for data subject access requests (currently £10). Any such request will normally be complied with within 40 days of receipt of the written request and, where appropriate, the fee.

In order to respond efficiently to subject access requests TrainerMaker needs to have in place appropriate records management practices.

## Section 11: Disclosure of Data

TrainerMaker must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff and students should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work related matter. The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of University business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the member of the University concerned.

This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

1. the individual has given their consent (eg a student/member of staff has consented to the University corresponding with a named third party);
2. where the disclosure is in the legitimate interests of the institution (eg disclosure to staff - personal information can be disclosed to other University employees if it is clear that those members of staff require the information to enable them to perform their jobs);
3. where the institution is legally obliged to disclose the data (eg immigration compliance, HESA and HESES returns, ethnic minority and disability monitoring);
4. where disclosure of data is required for the performance of a contract (eg informing a student's financial sponsor of course changes/withdrawal etc);
5. In exceptional circumstances, under the authorisation of the Chief Operating Officer, personal information may be disclosed to the police in writing where this is considered to be in public interest and for the prevention or detection of crime.

The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

* to safeguard national security\*;
* prevention or detection of crime including the apprehension or prosecution of offenders\*;
* assessment or collection of tax duty\*;
* discharge of regulatory functions (includes health, safety and welfare of persons at work)\*;
* to prevent serious harm to a third party;
* to protect the vital interests of the individual, this refers to life and death situations.

\* Requests must be supported by appropriate paperwork.

When members of staff receive enquiries as to whether a named individual is a member of the University, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (ie consent not required), the member of staff should decline to comment. Even confirming whether or not an individual is a member of the University may constitute an unauthorised disclosure.

Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request.

As an alternative to disclosing personal data, the University may offer to do one of the following:

* pass a message to the data subject asking them to contact the enquirer;
* accept an incoming email or other message and attempt to forward it to the data subject.

Please remember to inform the enquirer that such action will be taken conditionally: ie "if the person is a member of the University" to avoid confirming their membership of, their presence in or their absence from the institution.

Further information regarding the disclosure of personal information can be found in Appendices V ([student information](https://www.lboro.ac.uk/admin/ar/policy/dpact/disclosure/index.htm)) and VI ([telephone protocol](https://www.lboro.ac.uk/admin/ar/policy/dpact/telephone/index.htm)).

If in doubt, staff should seek advice from their University Data Protection Officer.

## Section 12: Retention and Disposal of Data

Personal data should not be retained for any longer than required. Considerable amounts of data are collected on current staff and students. However, once a member of staff or student has left the institution, it will not be necessary to retain all the information held on them.

### Students

In general, core information held in electronic student records (LUSI) will be kept indefinitely and includes name and address on entry and completion, programmes taken, assessment results, awards obtained. This enables the University to confirm awards (e.g. to future employers) and to issue replacement certificates and transcripts.

Schools should regularly review any locally held records on individual students in accordance with the [University's Records Retention Schedule](https://www.lboro.ac.uk/data-privacy/policiesandpractice/retentionschedule/).

### Staff

All core information will be retained for 6 years from the end of employment. Information relating to Income Tax, Statutory Maternity Pay etc will be retained for the statutory time period in the [Records Retention Schedule](https://www.lboro.ac.uk/data-privacy/policiesandpractice/retentionschedule/). Any employee personal data anywhere in University systems must be retained in compliance with the [Loughborough University Staff Data Privacy Notice on the HR website](https://www.lboro.ac.uk/services/hr/conditions-of-service/gdpr/).

Applications for posts within the University will be retained in iTrent for 12 months with the consent of the applicant.

### Disposal of Records

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (eg, shredding, disposal as confidential waste, secure electronic deletion).

## Section 13: Publication of University Information

All members of the University should note that the University publishes a number of items that include personal data, and will continue to do so. 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.
* 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 that their personal details in some of these categories remain confidential or are restricted to internal access. All individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, the University should comply with the request and ensure that appropriate action is taken.

## Section 14: Direct Marketing

Any School or Service that uses personal data for direct marketing purposes must inform data subjects of this at the time of collection of the data. Individuals must be provided with the opportunity to object to the use of their data for direct marketing purposes (eg an opt-out box on a form).

## Section 15: Use of CCTV

The University's use of CCTV is regulated by a separate Code of Practice.

For reasons of personal security and to protect University premises and the property of staff and students, close circuit television cameras are in operation in certain campus locations. The presence of these cameras may not be obvious. This policy determines that personal data obtained during monitoring will be processed as follows:

* any monitoring will be carried out only by a limited number of specified staff;
* the recordings will be accessed only by the Security Manager, the Deputy Security Manager, Security Supervisors and Security Control Room Operators;
* personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete;
* staff involved in monitoring will maintain confidentiality in respect of personal data.

## Section 16: 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 Data Protection Act 1998. 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](http://www.lboro.ac.uk/committees/ethics-approvals-human-participants/).

### Publication

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. Results of the research can be published on the web or otherwise sent outside the European Economic Area but if this includes any personal data, the specific consent of the data subject must, wherever possible, be obtained.

## Section 17: Appendices

More detailed guidance on the following issues has been published by the University:

* [Subject Access Request Procedure](http://www.lboro.ac.uk/admin/ar/policy/dpact/procsar/index.htm)
  + I: [Handling Subject Access Requests](https://www.lboro.ac.uk/admin/ar/policy/dpact/sareq/index.htm)
  + [II: Student Records Management in Academic Departments](https://www.lboro.ac.uk/admin/ar/policy/dpact/rmac/index.htm)
  + [III: Student Records Management in Support Service Sections](https://www.lboro.ac.uk/admin/ar/policy/dpact/rmsserv/index.htm)
  + [IV: Staff Records Management](https://www.lboro.ac.uk/services/hr/itrent/) [links to HR site]
  + [V: Disclosure of Student Information](https://www.lboro.ac.uk/admin/ar/policy/dpact/disclosure/index.htm)
  + [VI: Telephone Protocol for the Disclosure of Personal Information](https://www.lboro.ac.uk/admin/ar/policy/dpact/telephone/index.htm)
  + [VII: Records Retention Schedule](https://www.lboro.ac.uk/admin/ar/policy/dpact/recret/index.htm)
  + [VIII: Examinations and Assessment](https://www.lboro.ac.uk/admin/ar/policy/dpact/ea/index.htm)
  + [IX: References](https://www.lboro.ac.uk/admin/ar/policy/dpact/refs/index.htm)
  + [X: Photographs to be used in Publicity/Promotional Material](https://www.lboro.ac.uk/admin/ar/policy/dpact/photos/index.htm)

## Section 18: Further Information

Useful web addresses:

* [Information Commissioner's Webpage](https://ico.org.uk/)
* [HESA Data Protection](https://www.hesa.ac.uk/about/regulation/data-protection)
* [Ethical Advisory (Human Participants) Sub-Committee](http://www.lboro.ac.uk/committees/ethics-approvals-human-participants/) (Loughborough University)