THE UNIVERSITY OF LEEDS

Code of Practice on Data Protection

Set out below is the University's code of practice on data protection, which accords with the Data Protection Act 2018 (DPA) and takes into account the guidance published periodically by the Information Commissioner's Office.

The law

Data protection legislation encompasses the DPA and the General Data Protection Regulation. It requires that personal data is:

- processed fairly, lawfully and in a transparent manner;
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with these purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, up to date;
- not kept for longer than necessary; and
- kept safe and secure.

In addition, the University is also required to be able to evidence compliance with these principles.

When does the law apply?

It applies to all processing of personal data carried out for a University purpose, irrespective of whether the data is processed on non-University equipment or by third parties.

"Processing" encompasses the collection, recording, structuring, storage, adaptation or alteration, retrieval, use, making available, alignment or combination, restriction, erasure or destruction of personal data by either manual or automated means.

"Personal data" encompasses any information relating to a living individual 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 factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

In practical terms, it seems prudent to assume that anything which is recorded in relation to an individual may fall under the provisions of the legislation.

How does the University comply with the law?

The University takes seriously its responsibilities under data privacy legislation. It recognises that the mishandling of an individual's personal data my cause them distress or put them at risk. There are also legal, financial and reputational risks for the University if the personal data it is responsible for is not processed lawfully.

The University has to process information about its employees, students, alumni community and other individuals for administrative, research and general business functions. In accordance with the law, the University will advise individuals about the processing which is

taking place and the lawful bases under which it is being conducted. The University has a series of published documents in place which address its main processing activities:

- The Staff Privacy Notice
- The Student Privacy Notice
- The Student Contract
- The Alumni and Development Privacy Notice
- The Research Privacy Notice

Where processing of the personal data of external enquirers, or other users of the University's services, is necessary the University can, in most instances, rely on the provisions in the legislation to process for the performance of a contract, for legitimate interests or for a task carried out in the public interest. Processing activity which is not covered by one of the above will be addressed on a case-by-case basis with guidance from the Data Protection Officer.

Data security

All individuals with access to personal data must complete the mandatory Essentials training; those with access to confidential or special category personal data must also complete the Advanced training.

The University anticipates that the majority of the personal data for which it is responsible will be in electronic format and stored on its secure servers. Whilst the security of the campus network is the responsibility of the University, individuals are expected to take appropriate security precautions in respect of day-to-day PC usage; further detail is iterated in the University's Information Protection Policy.

Where personal data is kept in paper copy, individual owners are expected to take sensible precautions, including the use of locked drawers or filing cabinets.

Off-site use of personal data presents a potentially greater risk. Personal data should be only be taken off site when absolutely necessary and for the shortest time possible; laptops and pen drives which contain personal data should always be encrypted.

Sometimes it is necessary to share personal data outside the University, in which instance individuals should refer to the templates on the University's Data Protection website to ensure that the transfer is lawful and secure. Advice can also be sought from the Data Protection Officer.

Where personal data has been lost, or an individual believes that their University computer or its systems have been breached, the University protocol for reporting a breach must be followed; details can be found on the University's Data Protection website.

Retention of data

It is not in the interest either of individuals or the University to retain unnecessary or duplicative information. The University does have to retain some data relating to former staff and students partly in order to comply with statutory requirements but also as a way of maintaining a complete historical record. Nonetheless, it is University policy to discourage the retention of personal data within files for longer than is needed, and a retention schedule is available on the University's Data Protection website.

Individual rights

Subject to certain exemptions, individuals have numerous rights under data protection legislation to allow them to restrict, or to access the personal data that the University holds on them. If a member of staff receives such a request from an individual they must forward it to the Secretariat to be handled centrally.

Roles and responsibilities

The University

The University is the registered Data Controller and, as such, retains overall responsibility for the management and protection of the personal data under its control. In doing so it will ensure that:

- Appropriate policies and procedures are in place to facilitate compliance with data protection legislation.
- A Data Protection Officer is appointed to oversee compliance.
- People coming into contact with personal data have received adequate training and know where to seek advice.
- Appropriate technical and organisational measures are implemented to protect personal data.
- A record of processing activity across the institution is maintained.
- The ICO is notified of any data breaches as required.
- Appropriate measures are implemented to protect the rights of individuals.

Staff

All staff are required to:

- Undertake at least the Essentials training.
- Familiarise themselves with the relevant polices (including the use of personal data in research).
- Ensure that personal data is used appropriately and kept secure.
- Advise the Secretariat of any requests received in relation to individual rights under data protection legislation.
- Follow the appropriate reporting procedure in the event of a loss, or breach, of personal data.
- Ensure that the personal data about themselves which they provide to the University is up to date and accurate.

Students

All students are required to:

- Ensure that the personal data about themselves which they provide to the University is up to date and accurate.
- Where they come into contact with the personal data of others (including for use in research) they must abide by the University policies and procedures often, in the first instance, via conversation with their course leader/tutor.

Further information and advice is available either from your local Data Champion or from the University's designated Data Protection Officer, Alice Temple (on (0113) 34 37641 and on email a.c.temple@leeds.ac.uk).