WEDNESDAY 16 MAY 2018 • SUPPLEMENT (1) TO NO 5204 • VOL 148

Gazette
Supplement

University Policy on Data Protection

The following Policy on Data Protection was approved by Council on 14 May 2018 and will come into effect on 25 May 2018. This Policy supersedes the existing University policy on data protection.

1 Purpose and scope

This policy provides a framework for ensuring that the University meets its obligations under the General Data Protection Regulation (GDPR) and associated legislation[1] ('data privacy legislation').

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.

'*Personal data*' means any information relating to an identifiable living individual who can be identified from that data or from that data and other data. '*Processing*' means anything that is done with personal data, including collection, storage, use, disclosure and deletion.

More stringent conditions apply to the processing of special category personal data.

'*Special category*' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation.

This policy should be read in conjunction with the accompanying guidance, which provides further detail and advice on practical application, as well as any other documents that impose confidentiality or data management obligations in respect of information held by the University.

This policy does not cover the use of personal data by members of the University when acting in a private or non-University capacity.

2 Background

The processing of personal data underpins almost everything the University does. Without it, students cannot be admitted and taught; staff cannot be recruited; living individuals cannot be researched; and events cannot be organised for alumni or visitors.

We are responsible for handling people's most personal information. By not handling personal data properly, we could put individuals at risk.

There are also legal, financial and reputational risks for the University. For example:

- if we are not able to demonstrate that we have robust systems and processes in place to ensure we use personal data properly we might lose our ability to carry out research projects requiring access to personal data, particularly in the medical field;
- reputational damage from a breach may affect public confidence in our ability to handle personal information;
- the Information Commissioners Office (ICO), which enforces data privacy legislation, has the power to fine organisations up to 4% of global annual turnover for serious breaches.

3 Principles

The processing of personal data must comply with data privacy legislation and, in particular, the six data privacy principles. These principles are explained in detail in the University's Guidance on Data Protection[2].

In summary, they require 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 those 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, a new accountability principle requires us to be able to evidence compliance with these principles.

4 Aims and commitments

The University handles a large amount of personal data and takes seriously its responsibilities under data privacy legislation. It recognises that the mishandling of an individual's personal data may cause them distress or put them at risk of identity fraud. As a result, it is committed to:

- complying fully with data privacy legislation;
- where practicable, adhering to good practice, as issued by the ICO or other appropriate bodies; and

[1] This includes all legislation enacted in the UK in respect of the protection of personal data as well as the Privacy and Electronic Communications (EC Directive) Regulations 2003.

[2] www1.admin.ox.ac.uk/councilsec/compliance/gdpr/guidance

- handling an individual's personal data in a careful and considerate manner that recognises the importance of such information to their privacy and welfare.

The University seeks to achieve these aims by:

- ensuring that staff , students and other individuals who process data for University purposes are made aware of their individual responsibilities under data privacy legislation and how these apply to their areas of work. For example, employment contracts include a clause drawing the attention of the employee to data privacy legislation and the University's data protection policy;
- providing suitable training, guidance and advice. The University's online training course on data privacy and information security is available to all members of the University. The online course is supplemented by bespoke on-site training, where appropriate, along with regular talks and presentations at University conferences and departmental meetings;
- incorporating data privacy requirements into administrative procedures where these involve the processing of personal data, particularly in relation to major information systems (the concept of 'privacy by design');
- operating a centrally coordinated procedure (in order to ensure consistency) for the processing of subject access and other rights-based requests made by individuals; and
- investigating promptly any suspected breach of data privacy legislation; reporting it, where necessary, to the ICO; and seeking to learn any lessons from the incident in order to reduce the risk of reoccurrence.

5 Roles and responsibilities

Council

Council has executive responsibility for ensuring that the University complies with data privacy legislation.

It is supported by its General Purposes Committee, which is responsible for keeping under review the University's policies and compliance with legislation and regulatory requirements.

Data Protection Officer (DPO)

The DPO is responsible for monitoring internal compliance, advising on the University's data protection obligations and acting as a point of contact for individuals and the ICO.

Planning and Council Secretariat: Information Compliance Team

The Information Compliance Team is responsible for:

- establishing and maintaining policies and procedures at a central level to facilitate the University's compliance with data privacy legislation;
- establishing and maintaining guidance and training materials on data privacy legislation and specific compliance issues;
- supporting privacy-by-design and privacy impact assessments;
- responding to requests for advice from departments;
- coordinating a University-wide register exercise to capture the full range of processing that is carried out;
- complying with subject access and other rights-based requests made by individuals for copies of their personal data;
- investigating and responding to complaints regarding data privacy (including requests to cease the processing of personal data); and
- keeping records of personal data breaches, notifying the ICO of any significant breaches and responding to any requests that it may make for further information.

In fulfilling these responsibilities, the team may also involve, and draw on support from, representatives from sections, departments and divisions.

Heads of department (or equivalent)

Heads of department are responsible for ensuring that the processing of personal data in their department conforms to the requirements of data privacy legislation and this policy. In particular, they must ensure that:

- new and existing staff, visitors or third parties associated with the Department who are likely to process personal data are aware of their responsibilities under data privacy legislation. This includes drawing the attention of staff to the requirements of this policy, and ensuring that staff who have responsibility for handling personal data are provided with adequate training and, where appropriate, ensuring that job descriptions for members of staff or agreements with relevant third parties reference data privacy responsibilities;
- adequate records of processing activities are kept (for example, by undertaking register exercises);
- data protection requirements are embedded into systems and processes by adopting a 'privacy-by-design' approach and undertaking privacy impact assessments where appropriate;
- privacy notices are provided where data is collected directly from individuals or where data is used in non-standard ways;
- data sharing is conducted in accordance with University guidance;
- requests from the Information Compliance Team for information are complied with promptly;
- data privacy risks are included in the department's risk management framework and considered by senior management on a regular basis; and
- departmental policies and procedures are adopted where appropriate.

Others processing personal data for a University purpose eg staff, students and volunteers

Anyone who processes personal data for a University purpose is individually responsible for complying with data privacy legislation, this policy and any other policy, guidance, procedures and/or training introduced by the University to comply with data privacy legislation. For detailed guidance, they should refer to the University's Guidance on Data Protection[3] and any relevant departmental policies and procedures. In summary, they must ensure that they:

- only use personal data in ways people would expect and for the purposes for which it was collected;
- use a minimum amount of personal data and only hold it for as long as is strictly necessary;
- keep personal data up-to-date;
- keep personal data secure, in accordance with the University's Information Security Policy[4];
- do not disclose personal data to unauthorised persons, whether inside or outside the University;
- complete relevant training as required;
- report promptly any suspected breaches of data privacy legislation, in accordance with the procedure in section 6 below, and following any recommended next steps;
- seek advice from the Information Compliance Team where they are unsure how to comply with data privacy legislation; and

[3] www1.admin.ox.ac.uk/councilsec/compliance/gdpr/guidance
[4] www.infosec.ox.ac.uk/guidance-policy

- promptly respond to any requests from the Information Compliance Team in connection with subject access and other rights-based requests and complaints (and forward any such requests that are received directly to the Information Compliance Team promptly).

6 Breaches of data privacy legislation

The University will investigate incidents involving a possible breach of data privacy legislation in order to ensure that, where necessary, appropriate action is taken to mitigate the consequences and prevent a repetition of similar incidents in future. Depending on the nature and severity of the incident, it may also be necessary to notify the individuals affected and/or the ICO. A breach will occur where, for example, personal data is disclosed or made available to unauthorised persons or personal data is used in a way that the individual does not expect.

Incidents involving failures of IT systems or processes must be reported to the Oxford University Computer Emergency Response Team (OxCert) (oxcert@it.ox.ac.uk) within four working hours of discovery. OxCert will liaise, as appropriate, with the Information Compliance Team.

All other incidents must be reported directly to the Information Compliance Team (data.protection@admin.ox.ac.uk) at the earliest possible opportunity.

7 Compliance

The University regards any breach of data privacy legislation, this policy or any other policy and/or training introduced by the University from time to time to comply with data privacy legislation as a serious matter, which may result in disciplinary action. Depending on the nature of the breach, an individual may also find that they are personally liable (for example, it can be a criminal offence for a member of the University to disclose personal information unlawfully).

8 Further information

Questions about this policy and data privacy matters in general should be directed to the Information Compliance Team (data.protection@admin.ox.ac.uk).

Questions about information security should be directed to the Information Security Team (infosec@it.ox.ac.uk).

9 Review and development

This policy, and supporting guidance, will apply with effect from 25 May 2018. It will be reviewed during the 2018/19 academic year to take into account outstanding ICO guidance and the final form of national legislation underpinning the GDPR.

10 Related policies

This policy should be read in conjunction with related policies and regulations, including:

- the Information Security Policy[5]; and
- the Regulations relating to the use of Information Technology Facilities[6].

[5]www.infosec.ox.ac.uk/guidance-policy
[6]www.admin.ox.ac.uk/statutes/regulations/196-052.shtml