Data Protection Code of Practice

Data Protection legislation puts responsibilities and limitations on organisations and gives rights to individuals in respect of personal information. The legislation creates a number of offences with liability potentially falling on both the organisation and individuals dealing with personal data. Anyone breaking this code of practice may also find themselves subject to University disciplinary procedures.

The Open University complies with the Data Protection Act 1998. All members of staff and students under their supervision who process personal data must comply with the Data Protection principles as set out in the Act.

The Data Protection Principles

1. **Personal data shall be processed fairly and lawfully and shall not be processed unless certain conditions are met.**
   
   There are two parts to meeting the requirements of this principle. The first relates to fair obtaining which requires that certain information be made available when information is collected or obtained; and the second to the conditions for legitimising processing, one of which must be met. These include:
   
   - a. The data subject consenting to the processing
   - b. Processing for various contractual or legal and statutory purposes
   - c. Processing for the pursuit of the legitimate interests of the data controller (subject to conditions).

   Conditions for the processing of sensitive data are separately specified and are more rigorous and extensive. Sensitive data is defined in the Act as information relating to racial and ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, commission or alleged commission of any offence, and the outcome of any such offence.

2. **Personal data should be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.**
   
   Personal data obtained for one purpose may not be used for a completely different one without prior reference to the individual.

3. **Personal data shall be adequate, relevant and not excessive in relation to the purpose.**
   
   Only the minimum information to fulfil the purpose may be collected.

4. **Personal data shall be accurate and where necessary kept up to date.**
   
   Information quality and reliability are critical factors in effective data protection. Note that data are inaccurate if they are incorrect or misleading as to any matter of fact.

5. **Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes.**
   
   The University issues guidance and recommendations on the retention of records, including personal data.
6. **Personal data** (data relating to a living individual who can be identified) shall be processed in accordance with the rights of data subjects under the Act. These include the rights to:
   i. Subject access - see below.
   ii. Prevent processing likely to cause damage or distress.
   iii. Prevent processing for the purposes of direct marketing.
   iv. Have decisions made by automated means reviewed by a person
   v. Take action for compensation if damage is suffered by any contravention of the Act by the data controller.
   vi. Take action to rectify, block, erase or destroy inaccurate data.

7. **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**

It is important that security appropriate to the situation is in place and to remember that processing includes all operations concerning data from collecting and acquiring through to disposal. The University issues policies and guidelines on data security and these must be followed at all times.

8. **Personal data shall not be transferred to a country or territory outside the European Economic Area (the EU member States plus Iceland, Liechtenstein, Norway), 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.**

This includes electronic data that is stored on a server outside the EEA. Any information transferred to a country or territory that is not deemed ‘adequate’ by the UK Information Commissioner must only be done with the consent of the individual.

**Disclosures**

Personal data should not be disclosed to anyone outside the University (except with authorisation). The sending of personal data by email, a conference network, the Internet or file transfer constitutes a disclosure to the addressee and users must ensure that data subjects have been notified of these disclosures and that these disclosures comply with the Data Protection principles. Within the University, personal data must only be shared with other staff who need it in order to do their work. Personal data must be accessed for work purposes only and not used for any personal purposes. Requests from the Police or similar bodies for information about students should be referred to the Data Protection Coordinator. Requests for information about members of staff should be referred to the relevant HR manager.

**Identity Verification**

Before making changes or releasing details of personal records at the request of a data subject, the identity of the requester must be confirmed, as malicious or fraudulent requests are not unknown. Units have guidance on appropriate practice according to the nature of personal data processed within the Unit.

**Notification (Registration)**

The Open University is registered with the UK Information Commissioner. The University has provided a general description of the processing of personal data being carried out. It is recognised that staff, in the course of their OU work, will need to process personal data. In order to comply with requirements, the University’s Data Protection Co-ordinator needs to be aware of processing undertaken to ensure that the notification with the Information Commissioner is up to date and to consider any data protection implications. Any new databases or projects involving personal data must be notified to the University’s Data Protection Co-ordinator by completion of a questionnaire available on the University’s intranet [http://intranet6.open.ac.uk/governance/data-protection/ou-data-protection-procedures](http://intranet6.open.ac.uk/governance/data-protection/ou-data-protection-procedures). Separate advice for Associate Lecturers is contained in the Employment
Information section of TutorHome. If you have any doubts about whether a questionnaire is necessary, contact the Data Protection Co-ordinator.

**Subject Access**
An individual is entitled to be supplied with all the personal data held about them, subject to conditions. In view of the strict time limit imposed on organisations to comply, all such requests should be forwarded promptly to the Data Protection Co-ordinator, PO Box 497, The Open University, Walton Hall, MK7 6AT

**Complaints**
If an individual makes a complaint or is otherwise dissatisfied with the way their personal information is being processed by the University they should contact the Data Protection Coordinator at data-protection@open.ac.uk.

A complaint will be acknowledged and responded to in full within 28 calendar days and earlier where feasible. The outcome of a complaint will be that it is justified, part-justified or not justified. Where a subject can evidence a detriment or loss, the University will consider appropriate compensation. If they remain dissatisfied they have the right to make a complaint to the UK Information Commissioner www.ico.org.uk

**Further Advice and Information**
Staff must be aware of and observe the University’s Information Technology and Information Security Policies available on the IT intranet.

Queries relating to data protection can be directed to local unit Data Protection Liaison Officers or the University's Data Protection Co-ordinator.

Further information and advice can be obtained from:
http://intranet6.open.ac.uk/governance/data-protection/

The Data Protection Coordinator
EDIR, Academic Policy and Governance
Walton Hall
Milton Keynes

Email data-protection@open.ac.uk
Telephone 01908 653994

Authorised by University Secretary November 2008

Last reviewed August 2016
Reviewed annually