

UNIVERSITY OF ABERDEEN
POLICY ON DATA PROTECTION

The Data Protection Act 1998 (DPA) was passed in order to implement the EU Data Protection Directive (95/46/EC) and applies to all data relating to, and descriptive of, living individuals (defined by the Act as "personal data") which are held either electronically or in a structured manual filing system. The Act came into force on 1st March 2000. The University of Aberdeen is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of all data held by it which affects their privacy, whether in their personal or family life, business or professional capacity. The University adheres to the JISC Data Protection Code of Practice for the HE and FE Sectors published February 2009.

Data may only be processed in accordance with this policy and with the terms of the University's Notification to the Information Commissioner (Ref.: Z7266585), which sets out the purposes for which the University holds and processes personal data. Any breach of the policy may result in the University, as the registered *Data Controller*, being liable in law for the consequences of the breach. This liability may extend to the individual processing the data and his/her Head of School under certain circumstances.

PRINCIPLES

All data users must comply with the eight Data Protection Principles. The Principles define how data can be legally processed. 'Processing' includes obtaining, recording, holding or storing information and carrying out any operations on the data, including adaptation, alteration, use, disclosure, transfer, erasure, and destruction.

- Personal data shall be processed fairly and lawfully.
- Personal data shall be held only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed.
- Personal data shall be accurate and where necessary kept up to date.
- Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.
- Personal data shall be processed in accordance with the rights of data subject under the DPA.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of the data.
- 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.

The DPA defines both *personal data* and *sensitive personal data*. Data users must ensure that the necessary conditions are satisfied for the processing of personal data and in addition that the extra, more stringent, conditions are satisfied for the processing of sensitive personal data.

"Personal data" has a broad ranging definition and can include not only items such as home and work address, age, telephone number and schools attended but also photographs and other images, if focussed on an individual and disclosing information which is biographical in a significant sense. "Sensitive personal data" consists of racial/ethnic origin, political opinion, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life and criminal record.

STATUS OF THE POLICY

The policy was approved by the University Court on 25 May 2004 and updated September 2010. Any breach will be taken seriously and may result in action being taken under the appropriate disciplinary code.

RESPONSIBILITIES OF HEADS OF SCHOOLS, HEADS OF SECTION AND OTHER MANAGERS

Heads of School and managers of administrative and support services have a responsibility to ensure compliance with the Act and this Code, and to develop and encourage good information handling practices, within their areas of responsibility. All users of personal data within the University have a responsibility to ensure that they process the data in accordance with the eight Principles and other conditions set down in the DPA.

The University has issued detailed guidance to assist Heads of School and managers fulfil these obligations.

Heads of School may choose to delegate the management of, but not the responsibility for, Data Protection matters to another member or members of their staff.

The University will perform periodic audits to ensure compliance with this Code and the Act and to ensure that the notification is kept up-to-date.

HANDLING OF PERSONAL DATA BY STUDENTS

Academic and academic-related staff are responsible for the conduct in these matters of the students whom they supervise. The use of personal data by students is governed by the following:

- A student should only use personal data for a University-related purpose with the knowledge and express consent of an appropriate member of staff (normally, for a postgraduate, this would be the supervisor, and for an undergraduate the person responsible for teaching the relevant class/course).
- The use of University-notified personal data by students should be limited to the minimum consistent with the achievement of academic objectives. Wherever possible data should be de-personalised so that students are not able to identify the subject.

Use of a personal data by students is subject to the regulations set out below. The University's policy stated above and the regulations are based on the principle that students must only use personal data under the guidance of a member of staff. A breach of these regulations is an offence against University discipline.

- Students must not construct or maintain files of personal data for use in connection with their academic studies/research without the express authority of the appropriate member of staff.
- When giving such authority, the member of staff shall make the student aware of the requirements of the Data Protection Act and of the appropriate level of security arrangements which attach to the particular set of personal data.
- Students must abide by the Data Protection Principles and follow the instructions of the University in relation to any uses of personal data notified by the University.
- Research students must confirm when submitting their thesis that any personal data has been collected and processed in accordance with the Act.

ACCESS TO DATA

The Act gives data subjects a right to access to personal data held about them by the University, and allows the University to charge a fee for such access (up to a prescribed maximum). The University will however seek to take an approach which facilitates access to their personal data by individuals without them having to make formal subject access requests under the Act, whilst acting within the Data Protection Principles.

All formal subject access requests must be responded to within the 40-day period prescribed by the Act, and must be notified to the Data Protection Officer as soon as they are received. Any cases of doubt as to whether a request for access to personal data is a subject access request under the Act must be referred to the Data Protection Officer without delay.

The University will normally charge the prescribed maximum fee (currently £10) for subject access requests to personal data which is processed automatically or held in structured manual files.

From 1 January 2005, rights of access will be extended to data held in unstructured manual filing systems. However, the University will not be obliged to disclose such data unless the data subject can provide a description of it, nor if the costs of locating it exceed the maximum search costs allowed for under the Freedom of Information Act.

RETENTION OF DATA

Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. This applies to both electronic and non-electronic personal data. The University adheres to the model Action Plan for Records Management in Scottish HE & FE published February 2009. It intends to work towards a policy on retention that will allow users to apply a common standard University-wide in relation to disposal of personal data.

DATA TRANSFER

When personal data are transferred internally the recipient must only process the data in a manner consistent with the University's Notification and the original purpose for which the data was collected.

Personal data can only be transferred out of the European Economic Area under certain circumstances. The Act lists the factors to be considered to ensure an adequate level of protection for the data and some exemptions under which the data can be exported. Information published on the Web must be considered to be an export of data outside the EEA.

DATA SECURITY

All University users of personal data must ensure that all personal data they hold is kept securely. They must ensure that it is not disclosed to any unauthorised third party in any form either accidentally or otherwise.

DATA PROCESSING AND EXAMINATIONS

Current Senate policy is that while marks for in-course assessments and the final mark obtained for each course (which may optionally include General Papers taken at the end of the Final Honours Year) should be disclosed to students using the Common Assessment Scale, marks for individual elements of end-of-course assessment, such as examination questions, and the un-moderated marks awarded by individual examiners, should not. Accordingly, Schools wishing to use automated systems for processing examination results must inform the Data Protection Officer and comply with the processing windows that he prescribes. These normally run from the date to the first written exam at each diet to the final date prescribed by Senate for return of results. Marks may however be retained beyond this period for purposes of research and statistical analysis, provided that student identifiers have been removed.

Where exams are marked automatically, the Act requires that students are entitled to receive an explanation of the logic which underlies any decision to pass or fail them. It is however good practice that such results are reviewed by a member of academic staff or examiners' meeting before being signed off for publication.

It should be noted that while personal references contained in examination scripts are exempt from the Act, comments written on scripts may well fall within the definition of 'personal data' - particularly if commenting directly on the candidate.

DATA PROTECTION AND REFERENCES

References given are exempt from the Act: references received are not. However, before any disclosure is made regard must be had to the Data Protection rights of the provider of any reference, including any desire expressed by them in regard to disclosure.

DATA PROTECTION AND RESEARCH

Data collected for the purposes of research are covered by the Act. They will however be exempt from Subject Access if only intended for publication in such a way that individuals cannot be identified.

Staff collecting data for the purposes of research or consultancy are advised to incorporate an appropriate form of consent to process on any data collection form. Sample forms of words are available on the University's Data Protection Web Site.

DATA PROTECTION OFFICER

The University has notified the Office of the Information Commissioner of the purposes for which it processes personal data, Registration No. Z7266585. Questions related to the terms of the notification and other day to day matters on the operation of the policy and the Act can be dealt with by the Data Protection Officer for the University. The Data Protection Officer can be contacted by e-mail to dpa@abdn.ac.uk

Meta data

Updated by UMG: 30 May 2011

Updated by Court: 28 June 2011

File reference: N:\Information Compliance\Data Protection Act\DPA General\data protection policy_August 2010.docx