REGULATIONS

OXFORD BROOKES UNIVERSITY

E14 Data Protection Guidelines for Academic Staff

Data Protection Guidelines

1. Introduction

1.1 General

The Data Protection Act is concerned with the handling of personal information, covers both manual and electronic records and stipulates the setting of security standards. As part of the University's compliance with the legislation it has published an *Information Security Policy* and *E13 Data Protection Policy* and it is important that you make yourself familiar with them.

These guidelines are intended as a supplement to those policies. Further information and advice are available from the Information Compliance Team by email at info.sec@brookes.ac.uk

2. Standard Information

All staff process information about students on a regular basis, when marking registers, writing reports or references, or as part of a pastoral or academic supervisory role. The University will ensure through registration procedures that all students are notified of such processing, as required by the Act, and give their consent where necessary.

The information that staff deal with on a day-to-day basis is "standard" and covers categories such as:

- General personal details such as name and address.
- Details about class attendance, coursework marks, grades and comments.
- Notes of personal supervision, including matters of behaviour and discipline.
- Sponsorship details.

3. Sensitive Information

Information about a student's physical or mental health, ethnicity or race, political or religious views, trade union membership, sexual life, or criminal record is classified as sensitive information under the Data Protection Act.

Such information can only be collected and processed when permitted or required by law or with the student's express (written) consent. Examples would include:

- keeping of sick notes.
- recording information about dietary needs, for religious or health reasons, prior to taking students on a field trip.
- recording information that a student is pregnant, as part of pastoral duties.

Disclosure of such information without explicit consent is permitted only in exceptional circumstances, for example if the University is under a statutory obligation to make the disclosure or if the disclosure is in the vital interests of the student (information about a medical condition may be disclosed in "life or death" circumstances).

Sensitive information must be protected with a higher level of security. It is recommended that sensitive records are kept separately in a locked drawer or filing cabinet, or in a password protected computer file, or, if held on a mobile device, protected by encryption. If you (or one of your students) are holding, or intending to hold, sensitive personal information which is outside routine University processing, you should notify your manager or, if for research purposes, your research supervisor and your Faculty Research Ethics Team.

Every application to the University's Research Ethics Committee must include details of the measures to be taken to ensure the security of personal data.

4. Processing of Personal Information

Processing refers to any action involving personal information, including obtaining, viewing, copying, amending, adding, deleting, extracting, storing, disclosing or destroying information. When processing personal information, you must comply with the data protection principles, which are set out in the Data Protection Policy (regulation E13). In particular, you should ensure that records are:

- accurate.
- up-to-date.
- fairly and legally obtained.
- kept and disposed of safely.

For further details please refer to the University's record retention schedule.

5. Project and Research Supervisors

If you supervise students doing work that involves the processing of personal information, you should ensure that those students are aware of the Data Protection Principles, in particular, the requirements to notify and to obtain the data subject's consent where appropriate. Students should be referred to the Faculty Research Ethics Team or the Information Compliance Team for further information.

6. Handling Enquiries

When students ask to see information about themselves, you should, where possible, deal with these enquiries informally. If an informal response is not appropriate, you should advise the student to make a formal Subject Access Request under the Data Protection Act. Such requests should be directed to the Information Compliance Team. For all requests, both formal and informal, the information has to be provided within one-month of being received into the organisation.

You should not disclose personal information over the telephone unless you are able to validate the identity of the person making the request.

You may disclose personal information to other staff members who require the information in order to carry out their normal duties.

You should not disclose personal information to any third party, e.g., to a parent or sponsor, except with the consent of the student or where this is permitted or required by legislation.

In exceptional and urgent circumstances (e.g. cases where there are reasonable grounds for believing that an individual has become a danger to him/herself or others, or has committed / is about to commit a serious crime), you may release personal information directly to a law Team. Be sure to establish the identity of the law Team before releasing the information, and keep a record of the incident including name, date, circumstances and information disclosed. The details of any such disclosures should be reported to the Information Compliance Team.

7. Examination Marks

You should be aware that students are entitled to see preliminary marks and comments, which contribute to final assessments. SEC and MEC minutes will also be subject to access requests unless they are anonymised.

Similarly, when writing an academic reference, you should keep in mind that it may be subject to an access request by the student to the recipient.

The Academic Registry publishes procedures for the preparation of student references and the Supporting Students Handbook provides a template that you can work from.

8. Private Files

It is essential that relevant information is available to all University staff, so the case for holding "private", separate files has to be justified as being in the interest of the student (e.g., where the data is particularly sensitive). The information contained in them will still be subject to the student's right of access and you must ensure compliance with the notification requirements of the Act. Wherever possible, you should avoid duplication or fragmentation of student files.

9. Home Working

When working from home or on a laptop or tablet computer, you must maintain appropriate levels of security, including anti-virus (also known as anti-malware) software.

It is recommended that you ensure personal information is not stored on your domestic PC or computing device if this is used by other members of your family or household.

University data containing personal information should not be placed on portable devices unless it is necessary for a University business purpose and such processing has been authorised and the information is protected by encryption software.

If it is found necessary to work off site with University personal data then, in addition to encryption if held electronically, you must take sensible precautions to keep the data physically secure, for example, by using a lockable briefcase, storing data in the locked boot of a car while travelling, keeping the data in a secure location if held off site.

If you have concerns about the security of data, please consult the University Information Compliance Team for further guidance.

10. Exemption for Research Records

There is an exemption from some parts of the Data Protection Act where data is being processed for research and statistics. Information collected for the purpose of one piece of research can be used for other research, without breaching the "specified processing" principle (see the E13. Data Protection Policy), and can be kept indefinitely. For example, staff and students involved in academic research can keep records of questionnaires and contacts, so that the research can be re-visited at a later date, or so that, in support of a research project looking at an associated area, they can re-analyse the information. Researchers must ensure that the final results of the research do not identify the individual, or they will be subject to access requests under the Act.

This exemption is only applicable to academic research and cannot be relied on to prevent access to information about a particular individual, following research carried out for a redundancy or efficiency exercise, for example.

For further information about these regulations, please contact the Information Compliance Team via info.sec@brookes.ac.uk.