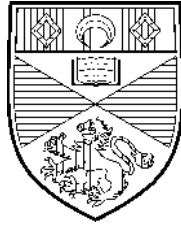


UNIVERSITY OF ST ANDREWS



DATA PROTECTION GUIDELINES FOR STAFF

AUGUST 2009

NB. These guidelines should be read in conjunction with the University's [‘Code of Practice: personal information about students’](#).

1 INTRODUCTION	2
2 GENERAL GUIDELINES	2
2.1 Collecting personal data	2
2.2 Security of personal data	3
2.3 Disclosing personal data.....	3
2.3.1 Relatives and guardians	3
2.3.2 The Police	4
2.3.3 Other government agencies.....	4
2.3.4 Embassies and High Commissions.....	4
2.3.5 Employment agencies and prospective employers	4
2.3.6 Telephone inquiries.....	4
3 EXAMINATIONS	5
3.1 Scripts	5
3.2 Comments on scripts.....	5
3.3 Publishing examination results	5
4 'CONFIDENTIAL' REFERENCES	5
4.1 Personal references.....	5
4.2 Requests for telephone or verbal references	6
4.3 Internal references	6
5 THE RIGHTS OF THE DATA SUBJECT	6
5.1 Subject access rights.....	6
5.1.1 Informal requests from an individual.....	7
5.1.2 Formal requests from an individual	7
5.1.3 Email.....	7
6 FURTHER INFORMATION	8

1 INTRODUCTION

The Data Protection Act 1998 (the Act) came into full force on 1 March 2000. It is much wider in scope than the 1984 Act which it replaced. In particular:

- The Act covers not only computerised data, but also manual records held in "relevant filing systems" [systems which allow for ordered retrieval, including card indexes etc].
- The definition of "data processing" has been broadened to include collection, recording, holding, retrieval, consultation, use and disclosure of data.
- Certain types of data are now classed as "sensitive" [data relating to ethnicity, political opinion, religion, trade union membership, health, sexuality or criminal record of the data subject] and the requirements for processing such data are more stringent.
- New conditions affect transfer of data to countries outside the European Economic Area – publishing on the World Wide Web may fall into this 'data transfer' category.

The intention of the Act is not to prevent data processing, but to ensure that it is done fairly and without adverse effect on the individual the data relates to. To this end, the Act lays down specific conditions for processing personal data.

A description of the Principles of the Act and definition of some of its terms can be found in Appendices A and B of the [University Data Protection Policy](#).

The University is legally obliged to comply with the provisions of the Data Protection Act. The following notes are for the guidance of staff in the University as to these obligations. It is not, however, possible to cover every activity that an individual or School/Unit might be involved in. If in doubt, please contact the University's Data Protection Co-ordinator [dataprot@st-andrews.ac.uk; tel 3528]

2 GENERAL GUIDELINES

NB. These guidelines should be read in conjunction with the University's "[Code of Practice: personal information about students](#)".

The guidelines are based on current interpretation of the provisions of the Act. They may therefore be reviewed as interpretations change and as case law emerges.

2.1 Collecting personal data

Schools and Units have to gather a certain amount of personal data [name, address, contact details etc] to carry out their normal functions. The Act requires, however, that only *necessary* data shall be collected. Schools and Units should therefore ensure that they only collect data that is necessary for the effective functioning of the unit. Procedures should be reviewed at intervals to ensure that this is the case, and that unnecessary information is not being requested or retained.

2.2 Security of personal data

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that access to the data must be restricted. All staff should ensure that:

- Manual records are kept in a locked filing cabinet or in a locked drawer. Care must be taken to ensure that manual records, e.g. staff or student files, or printouts containing personal data, are not left where they can be accessed by unauthorised staff.
- Computerised information is password-protected.
- Computer monitors are sited so that they are not visible except to authorised people. Screens should not be left unattended when personal data is being processed.
- Manual records, once they are no longer required, should be shredded or bagged and disposed of securely.
- Records, both manual and electronic should be retained/disposed of in accordance with the [Student Record Retention Schedule](#).

Staff should bear in mind that any personal data [either paper or electronic] taken away to be worked on at home needs to be treated with the same care for security.

2.3 Disclosing personal data

Students are private individuals and their data should not be disclosed to third parties without permission. In this context, "third parties" includes family members, friends, local authorities, government bodies and the police, unless disclosure is exempted by the Act or by other legislation.

There are certain circumstances where the Act permits release of data without express consent:

- for the purpose of protecting the vital interests of the individual [e.g., release of medical data where failure to do so could result in harm to, or the death of, the individual];
- for the prevention or detection of crime;
- for the apprehension or prosecution of offenders;
- for the discharge of regulatory functions, including securing the health, safety and welfare of persons at work;
- where the disclosure is required by legislation, by any rule of law, or by the order of a court.

2.3.1 Relatives and guardians

Parents may find it difficult to understand why a member of staff cannot discuss the academic progress of their child. Without the consent of the student involved, however, no such discussion is legally permissible. Written, rather than verbal, consent is recommended.

It is, however, perfectly allowable to discuss institutional procedures with parents. A member of staff may safely describe the procedures involved in re-sits, but not the reasons why Student X failed.

If there are circumstances where it is foreseeable that personal data might have to be released to parents [for instance if a student is spending a year abroad] written consent to this release should be obtained before the student leaves.

2.3.2 The Police

Disclosures to the Police are not compulsory except in cases where the institution is served with a Court Order requiring information. There is a limited exemption, however, which allows data to be disclosed for “the prevention or detection of crime” and “the apprehension or prosecution of offenders”.

Any requests for such information should be referred to the Registry.

2.3.3 Other government agencies

All requests should be referred to the Registry

2.3.4 Embassies and High Commissions

Any request from a foreign embassy for information about students or staff should be treated with great caution. It may be that the individual concerned has no desire for any contact with his home state or its representatives. This is for the individual concerned to decide.

If a School or Unit receives such a query about a student or graduate, they should request that it be made in writing and addressed to the Registry.

2.3.5 Employment agencies and prospective employers

Employment agencies or prospective employers may contact the University to verify such details about an individual as examination results and degree classifications.

The University is required by statute to maintain a register of all living graduates and their academic qualifications. Registry will therefore provide to such bodies confirmation of graduates' academic qualifications.

2.3.6 Telephone inquiries

Phone calls from a third party asking for information on a member of staff or student should be treated with caution.

Members of staff should:

- Explain that the University does not discuss individuals without the express permission of the individual concerned.
- **Not** confirm the presence or otherwise of the individual concerned.
- Offer to attempt to contact the person concerned and take details of the request for information, including the caller's number.
- Offer to phone the caller back if necessary [this offers some measure of authentication of the caller].
- Offer to accept a sealed envelope for the Department to try to forward to the individual concerned.

3 EXAMINATIONS

3.1 Scripts

Information recorded by candidates during examination (ie examination scripts) is specifically EXEMPTED from subject access provisions – in other words, the Data Protection Act does NOT entitle students to see [or have a copy of] the actual scripts. But see also: [Policy on Feedback to Students](#)

3.2 Comments on scripts

Examiners' [both internal and external] comments on the content of scripts are disclosable, whether recorded on the script or held separately. Students have the right to a copy of marks given, and any comments on which they were based.

This provision also applies to comments made by examiners of theses and dissertations, and to any notes made during a viva.

3.3 Publishing examination results

Schools and Departments should not post assessment results on public noticeboards. Students asking for advance notification should be informed that they must wait for the official notification which is sent to them individually by the Registry

4 'CONFIDENTIAL' REFERENCES

4.1 Personal references

Personal references supplied for specified purposes, including education, training or employment, are exempt from subject access. Thus, the writer of a 'confidential' reference for an individual cannot be required to disclose its contents in response to a data subject access request.

The exemption from disclosure does not, however, apply to the individual or organisation that receives the reference. They can be expected to disclose a reference, particularly if it is possible to conceal the identity of the referee [e.g., by blanking out their name, address, etc].

With this in mind, staff should:

- Always ensure the accuracy of any statements made in a reference.
- Ensure that any opinions expressed are justifiable and defensible.
- **NOT** supply sensitive data, [e.g. sickness, mental health problems] unless permission to do this has been explicitly given [in writing] by the data subject. 'I am not in a position to comment regarding X's health/sickness' would be a suitable response.
- **NOT** disclose any information if asked to give an unsolicited reference [for a person who has not, to your knowledge, cited your name as a referee.]
- Take particular care if asked to provide a reference for a student or other individual unknown to them and make it clear that their knowledge of the person is limited.
- Consider providing a strictly factual reference which makes no evaluative comments at all about the individual concerned.
- File copies of references provided and keep them securely.

4.2 Requests for telephone or verbal references

It is recommended that these are not routinely given. However, they would be acceptable where the data subject has specifically requested the referee to provide a reference that is required at short notice. If notes are kept of the conversation, these will constitute personal data.

The identity of the person requesting the reference should always be confirmed prior to disclosure. As a minimum security measure it is recommended that staff ring the enquirer back.

4.3 Internal references

Where internal references are concerned, the institution could be argued to be both the originator and the recipient. This would apply to references written on behalf of a member of staff applying for a post in another Unit/School or a reference supplied to the Promotions Board by a head of Unit/School.

The University would probably find it hard to justify refusal to disclose where a reference directly affected a candidate's career. If a data subject were to pursue a court case against the University, the reference would then most likely become disclosable anyway under the 'legal proceedings' exemption in the Act.

It could also be argued that internal references on members of staff may be more akin to staff appraisals or reports and therefore might not actually be exempted under the Act at all. There is as yet no case law on this.

Staff should therefore follow the same guidelines when writing internal references as they do when writing external ones.

5 THE RIGHTS OF THE DATA SUBJECT

Data subjects have the right to:

- Prevent processing if it is likely to cause them unwarranted damage or distress.
- Have any inaccuracies in their data corrected or erased.

If they can show damage they may:

- Receive compensation for loss of data or unauthorised disclosure.
- Receive compensation for inaccuracy.

5.1 Subject access rights

Under Section 7 of the Act data subjects have a right of access to any personal data held about them by a data controller.

This includes:

- Electronic and paper documents
- Data held in a database
- E-mail correspondence
- Any expression of opinion about the data subject

5.1.1 Informal requests from an individual

A School/Unit may choose to comply with an informal verbal request from an individual to see his or her files. This procedure is not without risk, however, and the School/Unit should bear in mind that:

- Such disclosures would be subject to obligations of confidentiality owed to third parties who may be mentioned in the documents.
- Units electing to respond independently to a request for 'All the information you have about me' run the risk of disclosing too little or too much information.
- The Act requires that data be kept secure. The School/Unit **MUST** ensure that the person requesting the information is in fact entitled to receive it.

It can be difficult to distinguish between an informal and a formal request for personal. If, for instance, an individual simply asks to see his marks, then ideally the Department in question will give him a copy and the he will be satisfied.

What can happen, however, is that the data subject may be dissatisfied, and will then ask for 'all the information you have about me.' At this point, the individual **MUST** be referred to the University's Data Protection Co-ordinator.

5.1.2 Formal requests from an individual

As soon as a request is made in writing [including by email] it **MUST** be referred to the University's Data Protection Co-ordinator in order to ensure that:

- The University complies with the requirement to reveal **ALL** the information [with very limited exceptions] that it holds about the data subject. The only way to achieve this is by a co-ordinated response.
- The University responds within the time constraints imposed by the Act
- The University discloses the information only to the person entitled to receive it.
- The University does not breach the confidentiality it may owe to third parties.
- The University is aware of, and documents, any instance of a Subject Access Request.

A Subject Access Request form is available from University's Data Protection Co-ordinator. This should be completed by the data subject and returned to:

Alison Aiton
Data Protection Co-ordinator
Business Improvements,
Butts Wynd
University of St Andrews

so that she can co-ordinate the response from the appropriate Schools/Units.

5.1.3 Email

It is important to remember that emails contain personal data in just the same way that a letter would. Moreover, an email does not have to be addressed to or received by the individual in question to be personal data about that individual – an email discussing a person may constitute personal data about him or her.

Email can also be very difficult to track down for any subject access request. Staff are advised, therefore, to adopt a policy of regularly deleting email from their desk-top machine – any email that needs to be retained can be printed out and filed.

6 FURTHER INFORMATION

Any member of staff requiring further information should contact:

Alison Aiton

Data Protection Co-ordinator

Business Improvements

Butts Wynd

Tel: 3528

[Email: dataprot@st-andrews.ac.uk](mailto:dataprot@st-andrews.ac.uk)
