Data Protection Guidelines for University Staff
(Appendix 4 of the University's Data Protection Policy)

---

1. **Introduction**

The revised Data Protection Act 1998, which is concerned with the handling of personal information, came fully into force on 1 March 2000. This Act is more stringent than the 1984 Act as, among other things, it covers both manual and electronic records and stipulates security standards. All staff share responsibility for processing data in accordance with the Data Protection Act.

2. **Standard Information**

Most staff process information about students on a regular basis e.g. taking registers, writing reports or references, data input to the University's central student information database (SITS), 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, address and date of birth;
- Details about class attendance, course work marks and grades and associated comments;
- Notes of personal supervision, including matters about 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 sensitive information under the Act. Such information can only be collected and processed as required by law, e.g. by the Children Act 1989, or with the student's **express (written) consent**. Examples:

- Disability records
- 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 consent is permitted only in "life or death" circumstances, e.g., if a student is unconscious, a tutor can tell medical staff that the student is pregnant or a Jehovah's Witness.

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, on an encrypted device or password-protected computer file. Where such information is required to be accessed from outside of the University's campuses, this should be by storing it in a network drive location and by using the remote access tools provided. The measures taken to safeguard such information should be implemented in accordance with the University of Chichester Electronic Information Security Policy. If you (or one of your students) are holding, or intending to hold, sensitive personal information which is outside standard University processing, e.g. for a research project, you should notify the Data Protection Officer.

4. **Processing of Personal Information**

Approved: Board of Governors – 25 November 2008
Policy & Appendices updated: December 2016

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. In particular, you should ensure that records are:

- Accurate;
- up-to-date; and
- fairly and legally obtained.

University data should not be made available to unauthorised persons, or for unauthorised activity. University data should never be stored on personal computers which are accessed by private individuals. Personal computers which use wireless connections should always use secure connections.

Emails and any electronic attachments that contain personal information must remain on University systems and not be sent or received on staff's personal (non-work) email accounts. Staff in this context includes any authorised person who has been provided with a system logon account.

5. **Exemption for Research Records**

There is an exemption under the Data Protection Act 1998 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 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 1998 Act.

This exemption is only applicable to academic research, i.e. the personal data are not processed to support measures or decisions relating to particular individuals; and are not processed in such a way that substantial damage or distress may be caused to the data subject(s), e.g. following research carried out for a redundancy or efficiency exercise.

6. **Research**

If you supervise students doing work which involves the processing of personal information, you should ensure that those students are aware of the Data Protection Principles and the University Ethics Policy. Students should be referred to the Data Protection Officer for further information.

Notwithstanding the exemptions referred to above, most of the data principles still apply to research which uses personal data, notably the requirement to keep data secure and for specific measures to be taken on each occasion data are collected for research purposes.

If the data are completely and genuinely anonymised and no "key" to the identity of the data subject is held by (or is likely to come into the possession of) a researcher, then the Data Protection Act does not apply, as such information is not considered to be "personal data" within the terms of the Act (i.e. data which relate to a living individual who can be identified from those data). However, if identification is at all possible, the Act still applies.

Generally, those collecting personal data as part of a research project must inform research subjects, as far as possible, and from the outset:

- the purpose of the research for which personal data about them will be collected;
- how their personal data will be used; and
- who will have access to their data.

It is expected that research applications will include an explanation and/or demonstration of how these measures will be taken.

It should also be noted that a research subject has the right to object to the processing of data on the grounds that such processing would cause them (or has caused them) significant damage or distress.

7. **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 Data Protection Officer.

You should not disclose personal information over the **telephone** unless you are able to validate the identity of the student.

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.

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 officer. Please contact the Data Protection Officer in such cases. Be sure to establish the identity of the law officer before releasing the information, and get an emailed or faxed copy of the request, and keep a record of the incident including name, date, circumstances and information disclosed.

8. **Examination Marks**

You should be aware that students are now entitled to see preliminary marks and comments, which contribute to final assessments. Committee 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.

9. **Private Files**

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) and the information contained in them will be subject to the student’s right of access. To ensure compliance with the notification requirements of the Act, you must inform the Data Protection Officer that you are holding such files. Wherever possible, you should avoid duplication or fragmentation of student files.

10. **Remote Access**

When working remotely on a University laptop, you should use the remote access services to store private and confidential information on the University's network drives. It is recommended that you do not work on USB memory sticks, or store any data on the laptop itself, as these can be lost and stolen. Private and Confidential University information should not be stored on any device not owned by the University, and even when using a University laptop:

- Special care should be taken in the transport of confidential information (particularly that which is personal information relating to people other than yourself).
- If it is absolutely necessary to do so, only ever carry paper files, laptops and memory sticks in a locked briefcase.
- If it is absolutely necessary to leave brief cases containing papers, laptops or memory sticks unattended, please store them in a locked office or locked away in your home.
- Never leave briefcases and laptops in your car.
- If it is absolutely necessary to use them, memory sticks must be encrypted and these should not in any case be used to store or transit confidential information.
- Emails that contain personal information must remain on University systems and must not be sent or received on staff's personal (non-work) email accounts.

For full information, please refer to the University's Electronic Information Security Policy: http://www.chi.ac.uk/about-us/how-we-work/policies/it-and-information-policies