



St George's, University of London

Guidelines on the Data Protection Act 1998



1. [Introduction](#)
2. [Basic Principles](#)
3. [Guidelines](#)
4. [What data may be held](#)
5. [Keeping data up-to-date and accurate](#)
6. [For how long should data be held](#)
7. [Data access](#)
8. [Data security](#)
9. [Transferring data outside the Institution](#)
10. [Informal data access requests](#)
11. [Formal data access requests](#)
12. [Research & Patient Data](#)
13. [References](#)
14. [Other Areas](#)

1. Introduction

These guidelines have been drawn up to give us a general, simple outline of the Data Protection Act 1998. Further details and advice about the Act can be obtained from the Institution's Data Protection Officer:

Andrew Judycki
Projects and Policies Manager

Tel: 020 8725 5639
Email: ajudycki@sgul.ac.uk

There is also a website giving further information on the Data Protection Act 1998

<http://www.ico.gov.uk/>

In terms of the Act, SGUL is the 'data controller.' The Institution's Data Protection Officer ensures that policies and procedures are in place to assist employees in complying with the Act on a day to day basis.

2. Basic Principles

The Data Protection Act 1998 concerns personal privacy.

Provided we adhere to the general principles embodied in the Act, it is not envisaged that the Act will cause us any difficulty.

In essence, we should all be:

- Open with individuals about information held about them.
- Very careful about passing that information to third parties.

The Act applies to data held in the Institution relating to living, identifiable individuals, whether the data is held on paper or on computer. Paper data must be part of a structured set of information about an individual. For example, this would include student files, staff files, a list of students taking a particular unit of study or a list of members of staff who had been on leave.

3. Guidelines

For some types of breach the Act provides for prosecution of those responsible and the right of the data subject to claim damages. All staff receive information on the Data Protection Act during the induction process. All staff are also asked to attend one of the regular training courses given by the Institution's Data Protection Officer.

Many of us will process data about staff and students on a regular basis such as:

- General personal details e.g. name and address.
- Details about class attendance, coursework marks and grades and associated comments.
- Notes on promotions, regradings etc.

Staff and students will have consented to the processing of this type of data when they joined the Institution, however, if you need to process the following 'sensitive' data you should contact the Data Protection Officer for advice.

- Physical or mental health

- Sexual life
- Political or religious views
- Trade union membership
- Ethnicity or race
- Details of any criminal offences or proceedings

We all have a duty to ensure that we comply with the data protection principles, in particular ensuring records are:

- Accurate
- Up-to-date
- Fair
- Kept and disposed of safely, and in accordance with SGUL policy.

4. What data may be held

4.1 Notification

The Institution's Data Protection Officer must notify the Information Commissioner's Office of the Institution's intention to process data. The Institution must indicate the type of data held, the purposes for which it is held, and those to whom it may be disclosed.

This Notification has been made and the Institution's registration number is Z5770328.

4.2 Content of files

When writing documents on paper or computer, we should bear in mind that individuals have the right to see their files. This includes e-mails and documents expressing opinions and intentions about an individual. Opinions expressed about individuals in documents should be justifiable and based on fact. For example, while it would be acceptable to give a reasoned, frank opinion of a student's performance, it would not be acceptable to express personal dislike or prejudice. Disclosed documents can be and have been used in court proceedings and in internal appeal and grievance hearings.

We should all note that e-mails can often be retrieved after they have been deleted - they differ from a telephone conversation in this way.

4.3 New data

If data comes into the Institution's possession, of which the individual is unaware and which the Institution chooses to retain, the individual should normally be informed of the fact and told why the Institution needs to retain the data. e.g. the instigation of criminal proceedings.

Any person responsible for new system developments should contact the Data Protection Officer to inform him whether or not the system to be developed or procured will hold personal data.

4.4 New purpose

Data obtained for one purpose may not be used for a different purpose without the individual's consent; for example a staff list may not be used for commercial mail shots.

4.5 All data

The Institution may hold data on an individual only with the individual's consent or with justification, as set out in the Act. For example, if it is necessary for the performance of the contract or for legal obligations. The simplest course is to obtain consent, and this should become standard good practice. Forms which gather data on an individual should give reasons why the information is required, and request consent under the Data Protection Act 1998. The Data Protection Officer can give advice on wording. This applies even if members of staff or students have signed a general Data Protection Act 1998 consent form when first arriving at the Institution.

4.6 Sensitive data

Additional conditions are imposed for sensitive data. Advice may be obtained from the Data Protection Officer.

Sensitive data is data concerning:

- Race
- political opinion
- religious belief
- trade union membership
- physical or mental health
- sexual life
- criminal offences

In cases of sensitive data, before processing can take place either the Institution must have the individual's explicit consent, or in addition to the standard justification, the retention and use must be necessary for some further reason, as set out in the Act. This might be, for example to:

- exercise a right or perform an obligation in relation to employment (e.g. keeping information about pregnancy to ensure fulfillment of health and safety obligations)
- protect vital interests when consent cannot be obtained (e.g. passing information about health problems to a paramedic following an accident)
- treat medical patients, when undertaken by a health professional or someone with an equivalent duty of confidentiality
- monitor equality of opportunity on racial grounds

Contracts of employment for staff and contracts with students will include permission for the Institution to process relevant sensitive information for proper purposes, for example about health, race or criminal convictions.

Photographs count as sensitive data, since they reveal information about the subject's race. Permission should always be obtained to keep, copy or use a photograph of an individual.

5. Keeping data up-to-date and accurate

If you are responsible for files or records please weed through them at appropriate regular intervals (probably annually) to ensure that the data held is up to date and accurate, and that it is still necessary to keep it. This is not only required under the Act, but is desirable in any event, for instance for writing references.

6. For how long should data be held?

We should not keep Data for longer than is necessary, and the Institution recommends disposal as set out below.

When paper documents are to be discarded, they should be shredded. For electronic data storage please consult Computing Services to ensure deletion of data is executed correctly.

Simply deleting data in a conventional way is almost always unsatisfactory.

6.1 Basic student information

The Institution keeps indefinitely a central record of basic staff & student information, sufficient to supply a transcript for any individual.

6.2 Staff and student files

Once a member of staff or student has left the Institution, his or her files can, save for a basic record of their employment or registration, be stored securely for up to ten years. If departments retain copies of documents from a file, these should be limited to necessary information, for example for the provision of references.

6.3 Applications

The Personnel Office will hold job shortlisting and interview notes for 1 year in case a dispute arises, for instance under the Race Relations Act, but not for longer than 1 year without the individual's permission. Departments may retain documentation from staff and student applicants on the same basis.

6.4 Archiving

- Consider drawing together all non-computerised records relating to a member of staff or student at their point of departure, for storage in a single departmental archive.
- Consider a two-stage archiving process. In the first instance, a full academic or conduct record should be retained for 6 years from a student or member of staff leaving the institution. Once that period has elapsed, the record should be reduced to its minimum amount: i.e. enough material to confirm the student's or staff member's personal details, class/work reference. All other materials should be destroyed, as arguably they are excessive and irrelevant to the intended purpose. Furthermore, sensitive data should be removed at this stage. It is advisable that we keep all records centrally in the Personnel Department.
- Consider moving away from paper and microfiche archives in favour of holding archive material in more easily accessible ways. e.g. electronic back-ups.
- Whatever the format of archive holdings, consider pruning previous archive material.
- Consider whether archive records are properly protected against loss or destruction, and are secure against accidental disclosure.

7. Data access

Only those with good reason to do so should see and process data. This is particularly important with sensitive data, for example relating to health. Sometimes it may be inappropriate to pass information within the Institution. Access to medical information should be restricted.

8. Data security

passed on improperly.

9. Transferring data outside the Institution

9.1 Information that a student is registered

Unless in a particular case there are good reasons to do otherwise (for example because of fear of violence from a former spouse), it will be made a condition of acceptance at the Institution that a student's registration is public knowledge. Thus, unless a student has been exempted by formal request, members of staff may confirm to an outside enquirer that a student is registered for a particular programme of study.

9.2 Sending data outside the European Economic Area (EEA)

The Act states that data should not be sent to countries outside the EEA which do not have an adequate level of data protection, unless the individual consents. The prudent course is to obtain the individual's consent before sending information outside the EEA.

9.3 Requests from the police

It is SGUL policy to co-operate with requests from the police, but steps should be taken first to ensure that requests are genuine. Disclosure is permitted under the Act for the prevention or detection of crime or the apprehension or prosecution of offenders. Requests by the police for information should be referred to the Institution's Director of Administration or the Data Protection Officer.

9.4 Requests from other official agencies

It may be proper to disclose information to the Inland Revenue or Contributions Agency, and advice should be obtained from the Data Protection Officer.

9.5 Other outside requests

Apart from requests from the police and some other agencies, and apart from confirmation that a student is registered, data should not be given to people outside the Institution (including parents of students) without consent or justification. If in doubt, advice should be sought from the Data Protection Officer. Any request from the media should be referred to the Public Relations Officer.

Requests from family or friends for a student's examination results should be refused, unless prior written permission has been received from the student.

9.6 Third party processors

If the Institution employs another party to deal with information about individuals, for example to prepare the Institution's payroll or to conduct a questionnaire, the Institution must have a written contract in place with the other party. The contract must stipulate that the third party may act only on the Institution's instructions, and must provide for appropriate security measures to prevent unauthorised disclosure.

10 Informal data access requests

Informal requests by an individual to see his or her files may be dealt with on that basis. You may wish to consult the Data Protection Officer first.

11. Formal data access requests

11.1 Requests

We all have the right to make an official written request to see the data held about us by the Institution. Such requests will be dealt with centrally by the Institution's Data Protection Officer. Subject to payment of a nominal fee and proof of identification the information should be provided within forty days. Where data is otherwise unintelligible, an explanation must be provided. Individuals are also entitled to know the purposes for which data is held, where it came from, and those to whom it may be sent.

11.2 Exemptions

The Act specifies some exceptions to the individual's rights. For example:

- An individual may not see statements of intention relating to pay or other negotiations, where disclosure might prejudice the negotiations;
- An individual may not see data relating to current management forecasting or planning, where disclosure might adversely affect the Institution's activities;
- If data discloses information about someone else, it should not be disclosed to the individual making the request unless the other person consents, or the document can be amended so he or she is not identified, or it is reasonable in all the circumstances to disclose without consent;
- An individual is not entitled to data where its compilation would involve "disproportionate effort"

11.3 Data access

Aside from the limited exceptions, an individual is entitled to see all information held about them by the Institution. To enable the Data Protection Officer to be sure that all the data on an individual has been accessed, it is important to be aware of what data you individually hold.

11.4 Alteration after request

Aside from routine amendments, data may not be erased or altered after the Data Protection Officer has received a request.

12 Research & Patient Data

12.1 Research Data

This is dealt with under section 33 of the Act. Further advice may be sought from the Data Protection Officer. Research data may be exempt from parts of the Act, provided it is:

- processed only for research purposes
- not processed to support measures or decisions with respect to particular individuals
- not likely to cause substantial damage or distress to any individual, and
- the results are not made available in such a form as to identify any individual

12.2 Patient Data

Patient Data is covered by the Trust's Data Protection Registration and as such it is the responsibility of the Trust to ensure that Patient Data is held in accordance with the Act. Anyone holding Patient Data should contact the Trust's Information Officer. It should be noted, however, that anyone holding private clinics with private patients, should themselves be registered as a Data Holder with the Information Commissioner's Office.

13 References

- References should be factually correct and state within what parameters the reference is given.
- Where opinions about a person's suitability are disclosed, we should be sure that our comments can be defended and justified on reasonable grounds. Statements should not be made which we are not qualified to make. For example, "I consider X to be well suited to the post for which he/she has applied and am happy to support his/her application" is better than "X will be a success in the post of ...".
- If asked to express an opinion on an issue about which you have a limited knowledge, e.g. honesty and integrity, an appropriate response might be, for example, "I know of nothing that would lead me to question X's honesty". Particular care should be taken if asked to provide a reference for a member of staff or student who is not known to us.
- Where reference forms request information relating to sensitive data, e.g. sickness, mental health problems, staff should not supply such data unless this is explicitly requested (in writing) by the data subject. 'I am not in a position to comment regarding X's health/sickness...' would be a suitable response.
- Employees should 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). Disclosure of data in the form of a reference should only take place either following confirmation of the employer's identity and the data subject's identity and application, or on specific request by the data subject.
- It is advisable to keep copies of any references provided, for a period of up to 6 months (in case of possible litigation from unsuccessful applicants).

14 Other areas

14.1 Examinations

Students are entitled to see their examiners' reports, including reports from the external examiners of research students, and examiners should be made aware of this. Examination marks may be seen.

14.2 Examination results

It will be a condition of acceptance as a student at the Institution that, unless for good reason, examination results may be made public on the results boards and at degree ceremonies.

14.4 Promotion and re-grading reports

The principles applying to references also apply to reports and assessments for promotion and re-grading.

14.5 Student debtors

Files may note the fact that a student owes money to the Institution, but access to the information will be restricted.

14.6 Alumni

Data held on students for the purpose of study will not automatically be used for fund-raising or friend-raising without permission. Permission should be sought from students as they leave the Institution.

14.7 Directories on the Internet

It will be made a condition of the Institution's contracts of employment that, unless there are good reasons to the contrary, work contact information and professional and research details may be included on the Intranet. Similarly it will be made a condition of contracts between students and the Institution that, unless there are good reasons to the contrary, their names, departments, programmes of study, and (where appropriate) research details may be included on the Intranet. This will be considered public knowledge. Certain items of personal contact information are made available on the Internet. The individual has control of the content and may request that no information is displayed. If an individual provides good reason to the Data Protection Officer why his or her entry should be withdrawn, the centrally maintained directory service will be revised to reflect this.

14.8 Temporary Staff

Please treat temporary staff in the same way as employees for the purposes of data protection. Although confidentiality is normally a clause of any employment agency contract, it is advisable to inform temporary staff, either verbally or by way of some prepared guidelines, of the requirement for confidentiality and the correct treatment of data under the Act. Please either give them a copy of the Institution's Data Protection Policy and these guidelines or let them have details of how they can locate them on the Institution's Intranet site www.sgul.ac.uk.