

HILLS ROAD SIXTH FORM COLLEGE

Data Protection Policy

Date approved by Resources Committee:

23rd November 2005

Post of member of staff responsible:

Assistant Principal (Resources)

1. Policy Statement

1.1 Hills Road Sixth Form College is committed to full compliance with the Data Protection Act 1998 (the Act) and recognises the responsibilities that the Act places on it to process and manage personal information in a fair and proper manner. The College has in place procedures to ensure practices exist to strike a balance between the College's needs and the individual's right to respect for their private life, confidentiality of data and the need to provide protection from unwanted or harmful uses of personal data.

1.2 In processing and managing data the College complies with the eight data protection principles of good practice noted in the Act. Specific procedures and processes are in place to ensure that the management of personal data adheres to these principles. The principles state that personal data shall be:

- obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
- obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
- adequate, relevant and not excessive for those purposes
- accurate and kept up to date
- processed in accordance with the data subject's rights
- kept safe from unauthorised access, accidental loss or destruction

and shall not be:

- kept for longer than is necessary
- transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

1.3 Rights under the Act are not subject to a minimum age requirement for applicants. Children can make a subject access request if they are capable of understanding the nature of the request. A parent or guardian can apply on the child's behalf if the child has given consent or the child is too young to have the understanding to make an application.

2. Responsibilities

- 2.1 The College is, as a corporate entity, the data controller under the Act. The Corporation is therefore ultimately responsible for implementation.
- 2.2 The College has three designated Data Controllers who are responsible for the general development, promotion and adherence to the College's Data protection policy and procedures. They are:
- Assistant Principal (Resources)
 - Assistant Principal (Support & Guidance)
 - Director of I.T.
- 2.3 The College has a valid notification in the data protection register that relates to processing information. This can be viewed at www.dpr.gov.uk. It is the responsibility of the Director of IT to ensure the registration is checked and updated on a regular basis.
- 2.4 Data protection compliance is ultimately the responsibility of all College staff. Individuals can be held legally responsible if they disclose personal information to any unauthorised third party. Serious breaches of data protection rules are considered to be a disciplinary matter.
- 2.5 In processing personal data staff are expected to:
- understand and adhere to the eight data protection principles set out in 1.2
 - manage personal data in accordance with the College's Data Protection policy, other relevant policies and procedures and the guidelines at appendix 1.
- 2.6 All staff and students are responsible for:
- checking that any personal information that they provide to the College is accurate and up to date
 - informing the College of any changes to information, which they have provided e.g. change of address
 - checking the information that the College will send out from time to time, giving details of information kept and processed
 - informing the College of any errors or changes. The College cannot be held responsible for any errors unless the staff member or student has informed the College of them.
- 2.7 Students who find themselves in a position where they are processing personal data about staff or other students (e.g. as a student representative on a College committee or team or as a member of the Student Council) must ensure that they comply with the College policy and the requirements of the Act.

3. Definition of Data

- 3.1 In the terms of the Act, data relates to an individual where the structure is such that information about the individual is readily accessed. The information may be held in manual form (e.g. as written notes relating to a person or as part of a filing system, including card index or filing cabinets structured by name, address or other identifier) or in a form capable of being processed electronically.
- 3.2 Personal data covers any data relating to a living individual (e.g. name, address, payroll details, examination results). Sensitive data form a subset of personal data that relate to a living person, recording such matters as racial or ethnic origin, political opinions, religious beliefs, trade union membership, health and criminal convictions.
- 3.3 The processing of data takes place whenever it is compiled, stored or otherwise operated upon. Disseminating the examination results of students involves processing data relating to each of them, as does giving and receiving personal references, producing agenda items or minutes for committees at which students are discussed as individuals, etc. Similarly, data about staff and applicants for posts are processed when they are committed to manual or electronic records held within the College.

4. Subject Consent

- 4.1 The Act does not allow an individual to prevent an organisation from making reasonable use of personal data in the interests of providing education or employment. For example, staff and students must expect certain information about them to be placed in the public domain. Permission to process staff or student data necessary in accordance with the College's contract to provide employment or education will be gained at the application and at the start of employment or student enrolment.
- 4.2 Sometimes it is necessary to process information about a person's physical and mental health, criminal convictions, race or ethnicity, sexual life, political or religious views and trade union membership details. This may be to ensure the College is a safe place for everyone, to assess suitability for employment or to operate other College policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for the College to do this. In certain circumstances, for example criminal background checks, the withholding of consent would result in the withdrawal of the offer of employment.

5. Rights to access information

- 5.1 Subject to a limited number of statutory restrictions, an individual or data subject (who could, for example, be a past or present student, a past or present member of staff or a current or previous applicant for a post) has a right to gain access to information that is kept about them.

A request to gain access should be made in writing, together with proof of identity, where relevant, to the Assistant Principal (Resources) in respect of staff and the Assistant Principal (Support and Guidance) for students. A fee of £10 may be charged on each occasion, although the College may choose to waive this.

The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within the statutory 40 calendar days provided the necessary fee (if not waived) has been received. Where a data controller reasonably requires additional information to deal with the subject access request, provided the data subjects is told what is required, the request does not have to be dealt with until this information is received..

Information released could include information that enables a third party to be identified. In such circumstances the College will balance the right of the individual to gain access against an expectation of privacy that may be held by the third party.

6. Retention of Data

6.1 16-19 students

6.1.1 Full information about 16-19 students will be kept for a maximum of ten years after they leave the College. This will include:

- name and address
- courses followed
- academic achievements
- copies of any reference written and
- destination information.

6.1.2 Basic details will be retained indefinitely. This will include:

- name, address and date of birth
- course information
- dates of attendance

6.1.3 Application forms of unsuccessful student applications will be held for a maximum of one year.

6.2 Adult students

6.2.1 Full information about adult students will be kept for a maximum of three years after they leave the College.

6.3 Staff

- 6.3.1 All information will be kept for twelve years after a member of staff leaves the College.
- 6.3.2 Where necessary information in respect of pensions, taxation, potential or current disputes or litigation regarding the employment and information required for job references will be kept for longer periods.
- 6.3.3 Basic details will be retained indefinitely. These will include:
- name, address and date of birth
 - dates employed
 - posts held
- 6.3.4 Data on unsuccessful applicants and unsolicited or speculative applicants for employment will be retained for one academic year.

7. Linked Statements, Policies and Procedures

- Acceptable use by students of College I.T. facilities
- Confidentiality between Teacher and Student
- Equality and Diversity
- Information Technology Security
- Staff References

8. Appendices

1. General guidelines
2. Retention of Records containing Personal Data

9. Further Guidance

Information Commissioners' website www.informationcommissioner.gov.uk

General Guidelines

1. Storing Personal Data

Personal data must be held securely. In the case of manual data this could be in filing cabinets, locked cupboards or rooms with access restricted to named individuals or categories of individual only. In the case of electronic information, access must be subject to reasonable controls including passwords and restricted access rights. Reasonable steps must be taken to detect and prevent unauthorised access. Regular backups should be taken to ensure that important data cannot be lost.

2. Disclosing Personal Data

Personal data should not generally be disclosed to third parties without the permission of the individual concerned. This covers both intentional disclosure and any disclosure that may happen by accident, for example someone having oversight of a monitor on which data is displayed. In this context, 'third parties' includes family members, friends, local authorities, government bodies and the police unless disclosure is exempted by the 1998 Act or by other legislation. Under certain circumstances, data may however be released. Note that among other circumstances 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 assessment or collection of tax
- where the disclosure is required whether as a statutory requirement or in response to a court order.

Most bodies that may request personal data in such circumstances should be able to provide documentary evidence to support their request. For example, many police forces have a specific procedure for requesting information in support of an ongoing investigation. The absence of such documentation, court order or a warrant may justify refusal to disclose personal data. Where there is a statutory obligation to disclose, the disclosure must be made. Requests of this nature should be passed to the Assistant Principal (Resources) for staff and the Assistant Principal (Support and Guidance) for students.

The College will make all reasonable efforts to obtain the consent of data subjects, staff and students, where non-sensitive personal data (including photographs) is to be used on the College internet and intranet web pages and in other publications where such use is not for the purposes of the normal organisational functioning and management of the institution for example general marketing purposes including publicity photographs, press releases, prospectus etc.

As a rule, personal or sensitive data should not be disclosed without the express consent of the individual concerned. Telephone disclosure is generally unsatisfactory, as verification of such details (and the identity of the enquirer) can be difficult. For example, a student's address, telephone number or e-mail should not be given to a telephone enquirer, even if the enquirer claims to be a close relative or friend. If a phone call is received from a third party requesting information on a member of staff or student, information about the individual should not be disclosed, however hard the caller may press, without the express permission of the individual concerned. Offer to attempt to contact the individual concerned and take details of the request for information, including the caller's number. If necessary ask them to put their request in writing and offer to accept a sealed envelope to forward to the individual concerned. Follow similar guidelines when dealing with written requests for information.

3. Protecting Third Parties

In meeting a data subject access request, it is important that personal data relating to other identifiable individuals mentioned in the documents (e.g. other staff or students) should not also be revealed unless permission for disclosure is given by the individual(s) concerned. Thus, a data subject enquirer has the right to see notes or comments relating to them that are held by the College in manual or electronic form, but the identity of the individual(s) who made those comments would not normally be revealed without their express permission.

Where it might be unrealistic to obtain consent, for example if the third party's whereabouts are unknown, a judgement should be taken about how reasonable it is in the circumstances to release the information. It may be necessary for example to edit the information to protect the third party's identity.

4. Disposal of Personal Data

Personal data should be disposed of when no longer needed for the effective functioning of the College and its members (see Appendix 2 for period of retention for records). The method of disposal should be appropriate to the sensitivity of the data. It is recommended that data on paper be shredded and that electronic data be permanently destroyed by reformatting or overwriting. Note that 'deleting' a computer file does not equate to destroying the data: such data can often be recovered. I.T. Services will provide advice as appropriate. Removable disks e.g. CD's, floppy disks, should be handed to IT Services for secure disposal.

5. Applications for Employment and Education

Notes made in the course of interviews constitute individual data and are therefore subject to access under the Act. They should be fair, reasonable and defensible. Interview notes relating to successful applicants may be retained while the individual is a member of the College, and hence be disclosable in response to a data subject request. Interview notes and all personal data

relating to unsuccessful applicants will be retained for up to one year after it has become clear that the individual will not be appointed or admitted to the College, but not retained for longer than necessary once that period has elapsed.

6. CCTV and similar surveillance equipment

The College employs closed-circuit television as part of its security systems and complies with the Code of Practice on the use of CCTV issued by the Office of the Information Commissioner.

Retention of Records containing Personal Data

Type of Record	Maintained by	Period of retention	Location of records	Reason for length of retention
Health and Safety records	Estates Bursar	10 years	Estates Bursar's office	Social Security (claims and payments) Regulations 1979, RIDDOR 1985
Ionising Radiation records	Estates Bursar	At least 50 years after last entry	Estates Bursar's office	Ionising Radiations Regulations 1985
Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 1999	Estates Bursar	40 years	Estates Bursar's office	Control of Substances Hazardous to Health Regulations 1999
Staff Personnel files	Personnel Administrator	Duration of individual's employment then archived for 12 years. Basic details comprising name, address, date of birth, dates employed and posts held, indefinitely	Resources office	References and potential litigation
Unsuccessful employment applications/interview notes and unsolicited/speculative applicants	Personnel Administrator	1 academic year	Resources office	Potential litigation Further employment vacancies
Facts relating to redundancies where less than 20 redundancies	Personnel Administrator	6 years from date of redundancy	Resources office	Time limits on litigation
Facts relating to redundancies where 20 or more redundancies	Personnel Administrator	12 years from the date of the redundancies	Resources office	Limitation Act 1980

Type of Record	Maintained by	Period of retention	Location of records	Reason for length of retention
Health records	Personnel Administrator	Duration of individual's employment then archived for 12 years	Resources office	Management of Health and Safety at Work regulations and potential litigation claims
Income tax and NI returns, including correspondence with tax office	Finance Bursar	At least 3 years after the end of the financial year to which the records relate	Bursary	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	Finance Bursar	At least 3 years after the end of the financial year to which the records relate	Bursary	Statutory Maternity Pay (General) regulations 1986
Statutory Sick Pay records and calculations	Finance Bursar	At least 3 years after the end of the financial year to which the records relate	Bursary	Statutory Sick Pay (General) Regulations 1982
Wages and salary records	Finance Bursar	6 years	Bursary	Taxes Management Act 1970
Adult Education student records	Adult Education Manager	3 years	Adult Education office Archive Room	Permits College to provide references for a reasonable length of time
16-19 Student records	Tutors	Maximum of 10 years from the date that the student leaves the College	Tutors' offices Staff Room Archive Room	Permits College to provide references for a reasonable length of time. Potential litigation claims
Accident register	Guidance officer	7 years	Guidance office Archive Room	Social Security (claims and payments) Regulations 1979; RIDDOR 1985
Student services <ul style="list-style-type: none"> • EMA • Access fund • childcare 	Guidance officer	Duration of student's enrolment then archived for 1 year	Guidance office	