Heythrop College
Data Protection Policy

Part One: Policy Context

Heythrop College is committed to a policy of protecting the rights and privacy of individuals (which includes students, staff and others) in accordance with the Data Protection Act. The College needs to process certain information about its staff, students and other individuals it has dealings with for administrative purposes (eg to recruit and pay staff, to run programmes of study, to record progress, to agree awards, to collect fees, and to comply with legal obligations to funding bodies and government). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The policy applies to all staff and students of the College. Any breach of the Data Protection Act 1998 or the College Data Protection Policy is considered to be an offence and in that event, Heythrop College disciplinary procedures may apply. As a matter of good practice, other parties and individuals working with the College, and who have access to personal information, will be expected to have read and comply with this policy.

Part Two: Background to the Data Protection Act 1998

The Data Protection Act 1998 enhances and widens the scope of the Data Protection Act 1984. Its purpose is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent.

Part Three: Definitions (Data Protection Act 1998)

Personal Data
Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, telephone number, id number. Also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

Sensitive Data
Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data are subject to much stricter conditions of processing.

Data Controller
Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

Data Subject
Any living individual who is the subject of personal data held by an organisation.

Processing
Any operation related to organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data Accessing, altering, adding to, merging, deleting data Retrieval, consultation or use of data Disclosure or otherwise making available of data.

Third Party
Any Individual/organisation other than the data subject, the data controller (College) or its agents.

Relevant Filing System
Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. Please note that this is the definition of "Relevant Filing System" in the Act. Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

Part Four: Responsibilities under the Data Protection Act

The College as a corporate body is the data controller under the new Act.

The Head of Student Services acts as the Data Protection Officer and is responsible for day-to-day data protection matters and for developing data protection awareness.

All staff in managerial roles are responsible for developing and encouraging good information handling practice within the College.

Compliance with data protection legislation is the responsibility of all members of the College who process personal information.

Members of the College are responsible for ensuring that any personal data supplied to the College are accurate and up-to-date.

Part Five: Notification to the Information Commissioner

Notification is the responsibility of the Data Protection Officer. Details of the College's notification are published on the Information Commissioner's website . Anyone who is, or intends, processing data for purposes not included in the College's Notification should seek advice from the Data Protection Officer.

Part Six: Data Protection Principles

All processing of personal data must be done in accordance with the eight data protection principles.

1. Personal data shall be processed fairly and lawfully.

Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

2. Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.

Data obtained for specified purposes must not be used for a purpose that differs from those.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.

Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data are given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.

4. Personal data shall be accurate and, where necessary, kept up to date.

Data, which are kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that data held by the College are accurate and up-to-date. Completion of an appropriate registration or application form etc will be taken as an indication that the data contained therein is accurate. Individuals should notify the College of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the College to ensure that any notification regarding change of circumstances is noted and acted upon.

5. Personal data shall be kept only for as long as necessary.

6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.

8. Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Data must not be transferred outside of the European Economic Area (EEA) - the EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual. Members of the College should be particularly aware of this when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.

Part Seven: Data Subject Rights

Data Subjects have the following rights regarding data processing, and the data that are recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing for purposes of direct marketing.
- To be informed about mechanics of automated decision taking process that will significantly affect them.
- To prevent processing likely to cause damage or distress.
- Not to have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the Act.
- To take action to rectify, block, erase or destroy inaccurate data.
- To request the Commissioner to assess whether any provision of the Act has been contravened.

Part Eight: Consent

Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. The College understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained where this data disclosure arises outside of routine data capture such as registration. In these circumstances, for example when a student discloses sensitive data to a member of staff not previously disclosed, the College's Consent Form for Disclosure of Sensitive Information (.doc) must be completed and signed by the member of staff and the discloser of information.

In most instances consent to process personal and sensitive data is obtained routinely by the College (eg when a student signs a registration form). Any College forms (whether paper-based or web-based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. It is particularly important to obtain specific consent if an individual's data are to be published on the Internet as such data can be accessed from all over the world. Therefore, not gaining consent could contravene the eighth data protection principle.

If an individual does not consent to certain types of processing (eg direct marketing), appropriate action must be taken to ensure that the processing does not take place.

If any member of the College is in any doubt about these matters, they should consult the College Data Protection Officer.

Part Nine: Data Security

All staff are responsible for ensuring that any personal data (on others) which they hold are kept securely and that they are not disclosed to any unauthorised third party.

All personal data should be accessible only to those who need to use it. Staff should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:

- in a lockable room with controlled access, or

- in a locked drawer or filing cabinet, or
- if computerised, password protected, or
- kept on disks which are themselves kept securely.

Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be wiped clean before disposal.

This policy also applies to staff and students who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and students should take particular care when processing personal data at home or in other locations outside the College campus.

Part Ten: Data Access Rights

Members of the College have the right to access any personal data which are held by the College in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by the College about that person.

Any individual who wishes to exercise this right should apply in writing to the Data Protection Officer. The College reserves the right to charge a fee for data subject access requests (currently £10). Any such request will normally be complied with within 40 days of receipt of the written request and, where appropriate, the fee.

In order to respond efficiently to subject access requests the College needs to have in place appropriate records management practices.

Part Eleven: Data Disclosure

The College must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff and students should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's

work details to someone who wished to contact them regarding a non-work related matter. The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of College business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the member of the College concerned.

This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

1. the individual has given their consent (eg a student/member of staff has consented to the College corresponding with a named third party);

2. where the disclosure is in the legitimate interests of the institution (eg disclosure to staff - personal information can be disclosed to other College employees if it is clear that those members of staff require the information to enable them to perform their jobs);

3. where the institution is legally obliged to disclose the data (eg HESA and HESES returns, ethnic minority and disability monitoring);

4. where disclosure of data is required for the performance of a contract (eg informing a student's LEA or sponsor of course changes/withdrawal etc).

The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security*;
- prevention or detection of crime including the apprehension or prosecution of offenders*;
- assessment or collection of tax duty*;
- discharge of regulatory functions (includes health, safety and welfare of persons at work)*;
- to prevent serious harm to a third party;
- to protect the vital interests of the individual, this refers to life and death situations.

* Requests must be supported by appropriate paperwork.

When members of staff receive enquiries as to whether a named individual is a member of the College, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (ie consent not required), the member of staff should decline to

comment. Even confirming whether or not an individual is a member of the College may constitute an unauthorised disclosure.

Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request.

As an alternative to disclosing personal data, the College may offer to do one of the following:

- pass a message to the data subject asking them to contact the enquirer;
- accept a sealed envelope/incoming email message and attempt to forward it to the data subject.

Please remember to inform the enquirer that such action will be taken conditionally: ie "if the person is a member of the College" to avoid confirming their membership of, their presence in or their absence from the institution.

Part Twelve: Retention and Disposal of Data

The College discourages the retention of personal data for longer than they are required. Considerable amounts of data are collected on current staff and students. However, once a member of staff or student has left the institution, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.

Students
In general, electronic student records containing information about individual students are kept indefinitely and information would typically include name and address on entry and completion, programmes taken, examination results, awards obtained.

The Registry and other departments should regularly review the personal files of individual students in accordance with the College's Student Records Retention Schedule.

College Staff
The College is working towards a records retention schedule that includes all of its sections but has commenced this project with the production of a Student Records Schedule and other sections will be added over the next few years – including for Human Resources.

Disposal of Records
Personal data must be disposed of in a way that protects the rights and privacy of data subjects (eg, shredding, disposal as confidential waste, secure electronic deletion).

Part Thirteen: Publication of College Information

All members of the College should note that the College publishes a number of items that include personal data, and will continue to do so. These personal data are:

- Internal Telephone Directory.
- Committee / other handbooks
- Student pass lists including grades.
- Information in prospectuses (including photographs), alumni newsletters, etc.
- Staff information on the College website / intranet (including photographs).

It is recognised that there might be occasions when a member of staff, a student, or a lay member of the College, requests that their personal details in some of these categories remain confidential or are restricted to internal access. All individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, the College should comply with the request and ensure that appropriate action is taken.

Part Fourteen: Direct Marketing

Any department or section that uses personal data for direct marketing purposes must inform data subjects of this at the time of collection of the data. Individuals must be provided with the opportunity to object to the use of their data for direct marketing purposes (eg an opt-out box on a form).

Useful references for further information:

- Information Commissioner's Webpage
- On-Line Data Protection Seminars (Information Commissioner's Office)
- HESA Data Protection
- JISC Senior Management Briefing Paper

A. M. Charles
5 December 2006