HARLOW COLLEGE

DATA PROTECTION POLICY

This Policy is issued by Harlow College in accordance with the Requirements of the Data Protection Act 1998.

Contents

Introduction

The College needs to keep certain information about employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be used fairly, stored safely and not disclosed to any other person unlawfully.

To do this, the College must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

The College and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the College has developed this Data Protection Policy.

Status of the Policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the College from time to time. Any failure to follow the policy can therefore result in disciplinary proceedings.

Any member of staff who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the Data Controller initially. If the matter is not resolved it should be raised as a formal grievance.

Notification of Data Held and Processed

All staff, students and other users are entitled to

- Know what information the College holds and processes about them and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the College is doing to comply with its obligations under the 1998 Act.

The College will update staff data when required or requested. Students' data are updated annually through the enrolment process or when notified of changes.

Responsibilities of Staff

- Checking that any information that they provide to the College in connection with their employment is accurate and up to date. Including marking, student data, etc
- Informing the College of any changes to information, which they have provided before changes, for example ,of address, bank information, next of kin, etc

- Checking the information that the College will send out from time to time, giving details of information kept and processed about staff.
- Informing the College of any errors or changes. The College cannot be held responsible for any errors unless the staff member has informed the College of them.

If and when, as part of their responsibilities, staff collect information about other people, (eg about students' course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff.

Data Security

All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.
- Where parents or carers ask for information on their son or daughter, this should only be disclosed with the authorisation of the young person themselves.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should be

- kept in a locked filing cabinet; or
- in a locked drawer; or
- if it is computerised, be password protected; or
- kept only on electronic media which is itself secure; or
- stored in a secure area of the network, only accessible by required staff (eg S drive).

Student Obligations

Students must ensure that all personal data provided to the College are accurate and up to date. They must ensure that changes of address, etc are notified to the student registration office/other person as appropriate.

Students who use the College computer facilities may, from time to time, process personal data (eg, an personal e-mail or document). If they do they must notify the Data Controller. Any student who requires further clarification about this should contact the Data Controller.

Rights to Access Information

Staff, students and other users of the College have the right to access any personal data that are being kept about them either on computer or in certain files. Any person who wishes to exercise this right should contact the college Data Controller (to request appropriate paperwork and authorisation – please note this may result in a charge) and hand it in to the reception, which will forward it to the Data Controller.

Students have access to view some of the data held about them through some automated systems, eg ProPortal.

In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing.

The College will make a charge of £10 per request. This may be waived or refunded at the Data Controller's discretion.

The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 calendar days unless there is good reason for delay, eg. a request falling over Christmas break or a large volume of requests.

In such cases, the reason for delay will be explained in writing to the data subject making the request.

Publication of College Information

Information that is already in the public domain is exempt from the 1998 Act. It is the College policy to make as much information public as possible, and in particular the following information will be available to the public for inspection:

- Names of College Governors and Register of interests of Governing Body members and senior staff with significant financial responsibilities (for inspection during office hours only)
- List of key staff
- Photographs of key staff
- Information on examination results
- The internal phone list may be a public document

Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the Data Controller.

Subject Consent

In many cases, the College can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to the College processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

Some jobs or courses will bring the applicants into contact with children, including young people under the age of 18 and vulnerable adults under 25. The College has a duty under the Children Act and other enactments to ensure that staff are suitable for the job, and students for the courses offered.

The College also has a duty of care to all staff and students and must therefore make sure that employees, and those who use the College facilities, do not pose a threat or danger to other users.

The College will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The College will only use the information in the protection of the health and safety of the individual, but will need consent to process, for example in the event of a medical emergency.

Prospective staff and students will be asked to sign a 'Consent to Process' as part of the college enrolment procedure regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form can result in the offer being withdrawn.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure the College is a safe place for everyone, 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. Offers of employment or course places may be withdrawn if an individual refuses to consent to this. More information about this is available from the Data Controller.

Safeguarding and Vital interest

Where sharing and recording of information is critical to prevent serious harm or distress, or in life threatening situations, the college will do this, however there will be no guarantee of confidentiality.

The information will still adhere to the data protection principles including, be accurate and up to date, shared securely and not kept for longer than necessary. Additionally any information will only be shared with the relevant authorities with the appropriate level of detail. This will range from no information being shared, flag indicating a safeguarding issue, basic summary or full disclosure. Where possible and appropriate the subject will be made aware of what sharing is likely to happen or in life threatening situations, the college will do this, however as per the college's safeguarding policy there is no guarantee of confidentiality.

The college has data sharing protocols with bodies such as, the local authority, funding bodies, awarding bodies and police authorities (not exhaustive). This is to provide information on student destinations, study programmes and funding, however it may also be used where there are serious safeguarding or criminal investigations.

The Data Controller and the Designated Data Controller/s

The College as a body corporate is the Data Controller under the Act, and the board is therefore ultimately responsible for implementation. However, there are designated Data Controllers dealing with day to day matters. The first point of contact for enquirers is:

Data Protection Controller: Debbie Sheridan Clerk to the Corporation

The Data Controller may either deal with the enquiry themselves for refer it to an appropriate member of staff.

With the introduction of the General Data Protection Regulation on 25th May 2018, conflict of interest means that many managers may not be able to take on this role going forward.

Examination Marks

Students will be entitled to information about their marks for both coursework and examinations. However, this may take longer than other information to provide. Please refer to the Examinations and assessment policies and procedures expected by Awarding bodies.

Retention of Data

The College will keep some forms of information for longer than others. Because of storage problems, information about students cannot be kept indefinitely, unless there are specific requests to do so. Many data retention periods are set by law or are a condition of funding.

Disposal of Data

When personal data is no longer required, or has passed its retention date, paper records must be shredded. This is disposed of using a reputable disposal contractor currently but may be brought on site at a later date.

Computerised records must be permanently deleted, with particular care taken that 'hidden' data cannot be recovered. The IT Helpdesk can advise on permanent deletion of computerised records. Hard drives are sent to a reputable disposal contractor that provides us with records of their destruction – see **Harlow College WEEE Collection Procedure**

Conclusion

Compliance with the 1998 Act is the responsibility of all members of the College. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the designated College Data Controller.

TRACKING and REFERENCE INFORMATION
Date Approved: Awaiting – February 2017
Review Date: 3 years from the date of approval
Author/Responsibility: Ben Nicholl
Equality Impact Assessment: n/a
List of related policies, procedures and other documents: All Harlow College policies, guidelines and briefings
Complaints: If you wish to submit a complaint about the application of this policy or the procedure of it, please send your request in accordance with the provisions of the Grievance Procedure.
Monitoring: The application of this policy and associated procedure will be monitored by HR Services
Easy reading: To receive this policy/procedure in a different format, please contact HR Services