

Partnerships: Data protection - guidance for students

The Data Protection Act uses terminology that requires some explanation

- Data:** any information that is processed either manually or electronically
- Personal data:** information about an identifiable living person
- Sensitive data:** personal data about racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical and mental health; gender preference; criminal convictions.
- Data subject:** the person identifiable from the data held
- Data controller:** the person who holds and processes personal data
- Data processing:** relates to anything which is done with or to data, including obtaining data; recording data; holding data; organising data; altering data; retrieving data; disclosing data; disposing of data.

Introduction

HEIs and their partner FECs need to collect and use personal data about their staff, students and other individuals. The process of the institutional transfer of HE students requires the use and processing of data used for:

- organisation and administration of courses
- admission of students
- monitoring of performance and achievements
- compliance with statutory obligations to funding bodies, government agencies and other bodies
- the provision of services
- recruitment and payment of staff
- monitoring health and safety
- research

In collecting and using data the university / college must comply with the Data Protection Act and its requirements regarding the processing of personal data. Under the act information must be collected and used fairly, stored safely, for no longer than is necessary and not disclosed to any person unlawfully. The act applies to data held in any form provided that it can be related to an individual; it covers computer records, e-mail, manual records and pictorial images. The act also provides that an individual about whom data is held has a right to request a copy of that data.

The following guidance notes outline the principles underpinning the act and some of the responsibilities it places on staff and students. The guidance cannot be exhaustive. If students have a particular query related to data protection not covered in these notes they should be able to seek further advice from a named source.

Principles

The Data Protection Act is based on eight principles. Compliance with the principles will ensure information is collected and used fairly, stored safely and not disclosed to any person unlawfully. The principles are that data shall be:

- obtained and processed fairly and lawfully
- obtained for a specified purpose and not processed in any manner incompatible with that purpose
- adequate, relevant and not excessive
- accurate and kept up to date
- not kept for longer than is necessary
- processed with due regard to data subjects rights
- kept safe from unauthorised access, accidental loss or damage
- not transferred to a country outside the European Union, unless that country has equivalent levels of protection for personal data.

Responsibility of staff towards students

It is quite likely that members of staff will process personal data on a regular basis. To ensure that the university / college is compliant with the Data Protection Act the consent of students to process personal data about them is obtained in principle at enrolment. Processing of sensitive personal data requires express consent.

Members of staff will ensure that any records or files they keep or process are compliant with the eight data protection principles of the act.

Members of staff processing data are prompted to ask themselves:

- do we need to record this data?
- does the data subject know that this data is held and for what reason?
- if the data is sensitive has the formal consent of the data subject been obtained?
- if the consent of the data subject is implicit are we satisfied that processing of the data is in their best interests?
- is the data accurate and how can this be checked?
- is the data held in a secure location such that no-one else will be able to access it without authorisation?
- how long do we need to keep the data?
- is there a mechanism for securely disposing of the data?

Responsibility of students

It is a requirement of the Data Protection Act that information processed about individuals is accurate. It is essential therefore that students keep their faculty or departmental office informed of changes to personal details such as address, name etc. The university / college is reliant on accurate personal data for communication with students on assessment results, award ceremonies and other matters.

Students undertaking project work or research may need to process personal data. The University is registered to undertake research and statistical analysis, but such work must be fully compliant with the principles of the act. Project supervisors at undergraduate level and directors of study at postgraduate level will offer advice about data protection issues.

Retention of data

The Data Protection Act requires that data is not kept for longer than is necessary and it is not in the university / college interest to retain unnecessary or duplicate information. However for certain types of record there are legislative requirements that oblige a particular retention period. For example, the Control of Substances Hazardous to Health Regulations requires that medical records are retained for 40 years. For student records including academic achievements and conduct the suggested retention period is six years from the date the student left the institution.

The university / college may keep a basic student record including a full transcript of academic achievements indefinitely.

Disclosure and security

University / college staff are frequently asked, by phone, e-mail, fax or letter, for information about students. It could be confirmation that they are registered, requests for an address, enquiries about results et al.

The guiding principle is that the university / college is not authorised to release any information about a student to anyone except that student unless:

- the student has given his/her explicit consent in writing to the disclosure; or
- the university / college is in receipt of an arrest warrant or a court order requiring disclosure; or
- a request has been received from the police, accompanied by a declaration form under the Data Protection Act confirming that the information sought is necessary for the prevention or detection of crime or the prosecution of offenders; or

- release of the information is an agreed pre-condition of student funding (e.g. attendance reported to Student Loan Company); this does not mean that all sponsors have rights to student information.

Unauthorised disclosure of information is not only a breach of the Data Protection Act, for which the university / college would be liable, but also breaches the undertaking of confidentiality to the student.

This applies even if the request for information comes from a relative, partner, colleague or close friend of the student. This may seem overly prescriptive – and can be difficult to explain to the person seeking the information, but it is what the university / college is obliged to do.

If a request for information on a student comes to a member of staff they will:

- explain that under the provisions of the Data Protection Act the university / college is required to keep all the information it holds about students confidential. The university / college cannot disclose any information – even whether the individual is a student – to anyone without either the student's written consent or a court order or formal police request
- explain that if the enquirer wants to contact an individual whom they believe to be a student, they should write in, and if that person is a student and the university / college has their address, it will be forwarded
- if the request is from the police, ask for a data protection declaration form, on receipt of which the university / college can disclose.

If a parent or partner says they have a right to the information because they are paying the fees, staff will explain that although the Local Education Authority may assess a student's fee contribution on the basis of a parents' or partner's income, the university / college contract is with the student. If a fee is not paid, the university / college cannot take action against a parent (or other sponsor) but only against the student.

If a parent or partner says that they know their son/daughter/partner would not mind/has asked them to act on their behalf/have always told them everything, staff will explain that sadly not every family is as close as theirs seems to be. Indeed there have regrettably been cases of people trying to obtain information under false pretences. Before the legislation, cases where information was disclosed in response to what appeared to be a genuine enquiry, caused students great distress. The University can disclose only if it gets written consent from the student.

A solicitor or barrister has no special status in these matters. Without a court order or the student's consent the university / college cannot disclose.

In addition to non-disclosure, all staff will take care to keep any information they hold on a student in a secure location and to maintain its confidentiality. This means care in the use of secure means of communication; keeping filing cabinets locked; switching off any computer holding personal data about individuals if a room is left unattended; ensuring information is not displayed on-screen or readable on a desk or in an in-tray when others are in the room; and shredding confidential papers or using secure disposal.

Access

Individuals have the right to access any personal data that the university / college keeps about them either on computer or in manual files. They are also entitled to access any recorded 'opinion about or intentions regarding a person'. As a consequence it is important that comments on personal files are fair, accurate, and justifiable and that staff would be comfortable to disclose comments. This extends to personal references. Though the university / college is not required to disclose the references it provides, the body in receipt of the reference is so required.

Most requests for information from students about themselves will be informal and addressed to particular departments, agencies or individuals such as finance, faculty offices, personal tutors etc. Data should be readily available on proof of identity with care taken that no data is released that would infringe the rights of third parties. However, under the act individuals have the right to access all the data the university / college keeps about them. Such a request should be formally made in writing to a named point of contact who will undertake an assessment of what files are pertinent. A fee of £10 will be charged and the university / college will provide the information within 40 days of receiving the fee. Individuals making a formal request will be asked to indicate which files in which areas they believe hold personal data about them. It is highly unlikely that any one individual could identify data in all files across the university / college. Willingness to specify information requirements and assist with defining the search profile greatly assists with meeting the individual's data requirements.

Exemptions

The university / college is entitled to withhold the following types of data:

- examination scripts
- confidential references – though the institution in receipt of a reference would have to provide access if requested under the rules governing normal subject access
- Legal professional privilege – relating to the release of personal data to a solicitor for the purpose of receiving legal advice
- management planning.

The university / college also deems it reasonable to expect that co-operation of a student in designating data requirements in any formal request for access.