Sharing of personal data

Introduction

It is sometimes necessary to share personal data or information with other University colleagues or with other organisations with which we have a relationship to ensure effective coordination and integration of services for staff and students.

This guidance details the requirements for sharing personal data in a safe and appropriate way in adherence with the Data Protection Act 1998.

As a data controller we notify the Information Commissioner's Office on an annual basis about the way in which we process personal information and we also provide examples of the types of sharing that is commonly undertaken.

Sharing information refers to the disclosure of information internally between different parts of the University or externally to a third party organisation.

Collecting personal data

The consent of the data subject should be obtained for collecting their personal data. Consent should be "informed" and "unambiguous". This means that the data subject needs to be told what information is to be shared, who it will be shared with, and why. They should be given the opportunity to object to the sharing of the data, or told that they can withdraw their consent at a later date. If consent is refused at any stage, a record should be kept of refusals, with dates. Explicit consent needs to be sought for the collection and processing of sensitive data.

It is acceptable to share information on a 'need to know' basis within the university where student information is required for someone to do their job. However, sensitive personal data (e.g. disability or health information) should not normally be shared without the explicit consent of the student – this means individuals must be fully aware of who the information will be shared with and should have given their agreement to this.

Reason or purpose for sharing data

Sharing personal data is not an automatic assumption and you must have a clear purpose for doing so e.g. achieving an objective that can only be achieved by sharing the information. Please see appendix 1 for a flowchart of questions .

Personal data can only be shared if there is a clear legal basis to do so or if the data subject has given their clear consent.

If you are required to share personal data you should be clear about the reasons for sharing the data, and what you intend to achieve by doing so. Ask yourself if the sharing of a particular piece of data is necessary for the working relationship.

When you collect any personal data you should always document the purpose you have for collecting the data, how it will be used, and with whom it will be shared. This should be reviewed and updated on a regular basis. Where databases of information are shared, responsibilities of staff should be made clear. Senior managers need to ensure compliance on their particular areas.

Any third party organisations with which you share information should separately, as data controllers, notify their purposes for processing data to the Information Commissioner. It may

be that the different parties process or use shared information for the same purposes. Or it may be that the parties have different purposes for processing or using information. If the purposes differ, each party must ensure that they are separately abiding by the principles of the Data Protection Act, and that they are specifying their purposes to the Information Commissioner. Using information for different purposes can be acceptable, as long as it is compatible with, or "not contradictory" to the original purpose for collection of personal data.

There is a "research" exemption of the Data Protection Act that does allow for the further processing of personal data, as long as it is only for research purposes (including statistical or historical purposes), and as long as the data is not processed to support measures or decisions about individuals; and is not processed in such a way that substantial damage or distress is likely to be caused to the individual.

Data Protection principles

There are eight data protection principles that must be adhered to in all cases when sharing any information:

Principle One
Personal data shall be processed fairly and lawfully and, shall not be processed unless: -
(a) at least one of the conditions in Schedule 2 (of the Act) is met, and
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 (of the Act) is also met.
Individuals should be made aware of which organisations are sharing their personal data and what their data is being used for.

Principle two
Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Principle three
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

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

Principle five
Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Principle six
Personal data shall be processed in accordance with the rights of data subjects under the Act.

Principle seven
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Principle eight
Personal data shall not be transferred to a country or 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.

Disclosure of personal information

When disclosing personal data to a third party you should, where practicable, keep a record of the date and details of the transfer of information.

Respect for confidentiality of data subjects

The law of confidence is a common law concept, which means that there is no Act setting it out, but that it has been developed by the courts over individual cases. A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. Examples may include safeguarding issues, health and wellbeing (including mental health), reporting of incidents and personal issues/circumstances. The duty of confidentiality applies whether the information has been requested or volunteered.

Data subjects sometimes allow us to gather sensitive information relating to their personal circumstances, health and wellbeing. They do so in confidence and they have the legitimate expectation that staff will respect their privacy and act appropriately.

Members of staff will often receive information of a personal and sensitive nature ranging from information required for administrative purposes related to application and enrolment to more sensitive information shared with tutors or wellbeing services. Compliance with confidentiality is the responsibility of all members of the University. Breaching confidentiality inappropriately could lead to legal action and loss of reputation.

Respecting confidentiality is essential. Without the trust that confidentiality brings, data subjects might not seek help and advice, or they might not give all the facts needed to provide for their education, health and wellbeing.

Staff must ensure that personal information is not disclosed to unauthorised third parties which includes family members, friends, Government bodies and in certain circumstances, the police. All staff should exercise caution when asked to disclose personal information held on a data subject to a third party.

In most instances, consent to process personal and sensitive information is obtained routinely e.g. when a student signs an enrolment form or when a member of staff starts employment. Agreement to process some specified classes of personal information is a condition of acceptance for students onto courses.

Personal information is usually disclosed with the consent of the data subject. When using, sharing or disclosing information you should:

- inform the person about possible uses of their information
- ask for consent before disclosing information that could identify them, if the information is needed for any other purpose
- disclose information that identifies the person only if this is necessary to achieve the purpose of the disclosure – in all other cases information should be anonymised before disclosing it
- keep disclosures to the minimum necessary and on a strictly ‘need to know’ basis

Sharing information with the right people can help to protect individuals from harm and ensure that they get the help they need. It can also reduce the number of times they are asked the same questions by different people.

If data subjects are able to take part in decision-making, you should explain why they need to share information, and ask for their consent. By asking for their consent to share relevant information, you are are showing respect and involving them in decisions about their education, health and wellbeing.

Sharing information without consent

There are certain circumstances when a data subject might not agree to disclosure but you still need to disclose information e.g.

- when there is an overriding public interest in the disclosure
- when it is judged that the disclosure is in the best interests of a student who does not have the maturity or understanding to make a decision a disclosure
- when disclosure is required by law
- when the data subject is at risk of sexual, physical or emotional abuse
- when the information would help in the prevention, detection or prosecution of serious crime
- when the data subject is involved in behaviour that might put them or others at risk of serious harm

Sharing information with the police

There is an exemption under the Data Protection Act which allows us to disclose information to the Police. This is known as the 'Section 29' exemption and covers disclosure for 'the prevention or detection of crime' and 'apprehension or prosecution of offenders'.

The police do occasionally ask for personal data as part of an inquiry but they don't have the automatic right to receive information about our staff or students. You should not be pressured into handing over personal information. There is a special process to allow the police to access personal data for certain crime-related purposes. Please contact the Data Protection Officer for further advice.

Sending personal data outside the European Economic Area (EEA)

The Act states that personal data should not be sent to countries outside the EEA that do not have an adequate level of data protection, unless:

- The data subject has given his/her consent to the transfer.
- The transfer is necessary for the performance of a contract between the data controller and the data subject; or a contract between the data controller and a third party which has been entered into at the request of the data subject, or is in the interests of the data subject.
- The transfer is necessary for legal proceedings or defending legal rights.
- The transfer is necessary for reasons of substantial public interest.
- The transfer is necessary to protect the vital interests of the data subject.
- The transfer is part of the personal data on a public register.
-

Data can be also be shared to countries outside the EEA where:

- The data is transferred to a company in the United States which has signed up to the a set of rules similar to those found in the UK's data protection law.
- The transfer is made under a contract which includes the model clauses adopted by the European Commission to ensure that there will be adequate safeguards for data transferred to a source outside the EEA.

Consent from the individual should be obtained before their personal data is sent outside the EEA.

Summary

When you share data you should be able to show that the sharing of data is lawful. You should be able to show that you have the correct powers for sharing the data, that you have considered the issues arising from the legislation, and that you understand the range of circumstances in which the transfer of information may be legitimate. If you have any queries about whether or not to share personal data please contact the Data Protection Officer, Teresa Kelly on ext 16018.

Author: Teresa Kelly, Data Protection Officer
Date: May 2016
Approved by Information Governance Group on 22 June 2016

Flow chart of when and how to share information