Right of Access to Personal Data

Contents

A. Right of Access

What are Data Subject Access Requests?

Data protection legislation gives individuals (data subjects) a number of rights including the right to access the personal data that an organisation holds about them.

The purpose is so that they are aware of and can verify the lawfulness of the processing of their personal data.

If an individual makes a request to view their own information, it is known as a "Data Subject Access Request". The right of access extends to all information held on an individual (e.g. enquirers, applicants, students and staff) and includes student record files, interview notes and emails referring to the individual.

A request can be very broad such as, 'give me a copy of all the information you hold about me', or it can be very precise, such as 'give me a copy of the letter you wrote about me yesterday'.

How a Subject Access Request should be made

- it is recommended that the request is made in writing using the online Data Request Form available through this link: https://goo.gl/cKb1m2
- information to verify who they are needs to be provided (to eliminate risk of unauthorised disclosure)
- appropriate information to help the University to locate the information requested needs to be provided.

How should the University respond to a Subject Access Request?

The information requested must be provided to the requester without delay and at the latest within one month of receipt of the request.

In some circumstances it is possible to extend the period of compliance by a further two months, for example, where requests are complex or numerous. If this is the case, the individual should be informed within one month of the receipt of the request and it should be explained why the extension is necessary.

Simple Requests

Published date: June 2023
Review date: May 2024

The majority of requests received by the University are likely to be from students asking for copies of a specific document(s). These will usually be located from a single source, typically from the central student file, e.g. transcript of results and will not involve the disclosure of information relating to a third party. However, subject access requests may be received from enquirers, applicants, students or staff and depending on the subject the request will be automatically sent to the following departments:

Former or current students - Student Administration

Former or current staff – Human Resources

Other – Data Protection Officer / relevant department

The request should be handled directly by the relevant department as above.

- confirm the identity of the data subject e.g. ascertain date of birth, course studied etc. (see point 3 below);
- check that there is no inadvertent release of third party information about another data subject as part of the request;
- if the data subject (student) is registered with the University as part of a collaborative arrangement, check which partner (institution) is responsible for subject access requests;
- release the information e.g. copy of a document to the data subject within one month.

Where a member of staff is in doubt about how to proceed with a Data Subject Access Request they should contact their department Data Champion or the university's Data Protection Officer.

Complex Requests

There may be some instances when a request for information is more complex and will need to involve the Data Protection Officer to ensure a coordinated response. Examples of situations where more complex requests might arise include:

- request involves locating information from multiple sources;
- request involves the release of contentious information;
- request is one in a series of requests from the same individual.

In such cases, the request must involve the head of department and the university's Data Protection Officer.

B. Third Party Data Requests

Personal data should not be disclosed to anyone including third parties such as parents and other family members and friends of the data subject (enquirer, applicant, student or staff) unless:

- written consent from the data subject is sought and obtained;
- consent has not been obtained but the circumstances are urgent and/or pressing and the vital interests of the data subject would be protected by disclosure (during an emergency, for example).

The University is obliged in certain circumstances to disclose personal data to third parties, for example, HESA and other government, regulatory and professional bodies and the police etc. The legal basis for disclosure in these circumstances is not related to the right of access and information in relation to routine disclosures of personal data is available in the University privacy policies.

How should the University respond to a Third Party Request?

If the request to disclose is from a third party and you are unable to obtain consent from the individual involved, you are advised to discuss the request with your Data Protection Officer in the first instance. The Data Protection Officer will consider the impact on the third party of the disclosure, and the impact on the data subject of the disclosure being withheld. Decisions will be made on a case by case basis.

C. Verifying the identity of the data subject or third party

It is important that you do not send copies of personal information to people who are not the data subject or third parties who are not among those for which consent is in place. The University is required to take 'reasonable measures' to verify the identity of a data subject/third party. You can often verify their identity from their circumstances, such as their address or signature. If you require further verification of the data subject's identity you can, for example:

- Telephone the individual and ask them two questions based on the information you hold about them, ask so as to confirm their identity.
- Write to the individual and ask them to send you a photocopy of their passport or drivers license.

D. Screening the information

Not all personal information can be disclosed. Once the information that is held about a data subject is collected together it must be examined in detail to establish if it should be disclosed. This must be done on a case-by-case basis for each individual piece of information. In some situations only parts of particular documents can be disclosed.

When responding to a subject access request or third party request it may be necessary to blank out [redact] parts of a document which should not be disclosed e.g. duplicate records, remove names of other individuals or unrelated sensitive information from emails etc.

For hard copy documents:

- Print out the document or, if it is a paper record, make a photocopy.
- Using a black marker pen, blank out the exempt information.
- Make a photocopy of the blanked out version. This is the copy that will go to the person making the request.

For electronic documents:

- Using the highlighter tool, highlight the exempt information in black.
- Save the blanked out version as a separate copy.
- Print out the document and send to the data subject/third party - do not send the document in electronic format if it is possible that the highlighting could be removed.

E. Keep a record

You need to keep a record for management purposes and log any queries in the request monitoring database. Create a file for each subject access request/third party request and store the following:

- Copies of the correspondence between the University and the data subject/ third party, and between the University and any other parties.
- A record of any telephone conversation used to verify the identity of the data subject/ third party.
- A record of your decisions and how you came to those decisions.
- Copies of the information sent to the data subject/third party. For example, if the information was anonymised, keep a copy of the anonymised version that was sent to the data subject.
- The file should be kept for a period of time in line with the University records retention schedule and then securely destroyed.

F. Evaluation and review

This policy will be formally reviewed every year by the Data Protection Officer and the relevant department(s) within the University. In addition, the effectiveness of this Policy will be monitored as necessary on an on-going basis to ensure it is compliant with relevant legislation.

This policy was last updated in May 2023.