Responding to Subject Access Requests (SARs)

This guidance aims to inform staff about:
- **What a Subject Access Request is**
- **Who can make a Subject Access Request**
- **What to do if you are contacted in relation to a Subject Access Request**
- **Information that may be exempt from disclosure**
- **Consequences of not following this guidance**
- **Help and support available to staff responding to Subject Access Request**

**What is a Subject Access Request and who can make one?**

The Data Protection Act applies to living, identifiable individuals. It gives such individuals the right to be told what ‘personal data’ an organisation is processing about them and, unless an exemption applies, to receive a copy of that information. They do this by making a data subject access request, which might be received by any member of staff. The request must be in writing (including e-mails and faxes), so if someone makes a subject access request by telephone or in person you should ask them to put it in writing using the form available here: http://www.nottingham.ac.uk/asd/Data%20protection.htm

The 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 (‘give me a copy of the letter you wrote about me yesterday’). The University must respond to such requests within 40 calendar days. Data subjects have the right to compensation in the event they are damaged by a contravention of the Act, for example if we fail to supply them with the information they request (unless exemptions apply to that information), within the 40 day time limit and their interests suffer as a result.

**If you are contacted in relation to a Subject Access Request**

When the Governance and Logistics Team receives a SAR they usually have to contact several different areas of the University to gather the information requested. In some cases it necessary to ask individual members of staff to look through their files, both paper and electronic.

Staff who have been asked to search their files should first check to see if the material they are being requested to search for is held in a “relevant filing system”. It is a ‘relevant filing system’ if the information is filed in a file with an index, contents list or other means of finding pieces of information. A file about a specific aspect of the University’s interaction with an individual is a ‘relevant filing system’, for example a file called ‘Dr X’s leave’ or ‘Dr X’s research’ or ‘Meeting about Dr X’. A general file about a particular subject, such as the payment of expenses, is a ‘relevant filing system’ if it has a sub section dedicated to Dr X or if the papers in the file are kept in alphabetical order so that you can go straight to a set of papers about Dr X.

The Governance Team can provide additional guidance on searching email and other electronic records for staff who would find it helpful. All records held by staff in their capacity as University employees are potentially disclosable. This includes records that are held on home PCs.
Accessing deleted and archived emails

With regards to deletion of email, Within Outlook you have two different types of message, those under 30 days which are stored in Exchange and these can be deleted and then the systems purges the deleted items in Outlook every 7 days, these are then moved to a safe area on Exchange and can be recovered for a further 21 days. People can check their deleted items themselves and they can also check the safe area by selecting deleted items in Outlook and then clicking the tools menu and selecting recover deleted items. The second type of messages is the archived messages these can be searched via Outlook. However, there is a stub in Outlook for all archived messages, these can be deleted by the customer via Outlook, but the archived message stays in the archive indefinitely or until the archive account is deleted. These can be searched by selecting the "Search Vaults" icon on the Outlook toolbar.

Information exempt from disclosure

In some, limited cases, information may be exempt from disclosure; (a list of possible exemptions is given at the end of this document). The decision on whether an exemption applies must be taken on a case-by-case basis for each individual piece of information. In some cases only parts of particular documents may need to be disclosed. The Governance and Logistics Team encourages staff they have contacted in relation to a SAR to provide the Team with all potentially relevant material so that a decision can be made on whether an exemption can be applied.

Consequences of not following this guidance

Staff are reminded that they must not destroy or refuse to disclose records because they would be embarrassing to disclose: this is a criminal offence if it is done after you know a SAR has been made.

As information is gathered material which does not reflect favourably on the University or individuals may be uncovered. For example, documents which show that standard procedures have not been followed, or documents which may cause offence to the data subject. These documents must be disclosed.

Data subjects may complain to the Information Commissioner about any decision we make regarding the disclosure or non-disclosure of information. The Information Commissioner may serve an enforcement notice ordering us to release the information. Any individual within the University who fails to release information after an enforcement notice has been served may be fined up to £5,000, and will have a criminal record.

Therefore, it is important that we disclose all of the information that the data subject has requested but only that information which is liable for disclosure. We must do this within the 40 day time limit. In any dispute it is important that the University is able to demonstrate that normal practice was followed. This guidance represents normal practice.

Help and support available

The Governance and Logistics Team can provide advice on responding to SARs, searching records and applying exemptions. Staff are encouraged to contact the Team to discuss any queries they have relating to both specific SARs and Data Protection.

Exemptions to the right of subject access:
The Act specifies a number of exemptions to the right of subject access. These include

**Crime and Taxation** (Section 29) - i.e. where personal data is processed:

- for the prevention or detection of crime
- for the apprehension or prosecution of offenders
- for the assessment or collection of any tax or duty or of any imposition of a similar nature.

**Research, history and statistics** (Section 33) - the exemption applies only if:

- the results of the research or any resulting statistics do not identify data subjects
- the data is not processed to support measures or decisions with respect to particular individuals
- the processing of data for research will not cause substantial damage and distress to any individual; and
- the data is otherwise processed in accordance with the Act

**Confidential references** given by the data controller (Schedule 7 Paragraph 1) - although references received should be disclosed in the event of a subject access request.

**Management forecasts/management planning** (Schedule 7 Paragraph 5) - where personal data is processed for the purposes of management forecasting or management planning and where subject access would be likely to prejudice the conduct of the business or other activity of the data controller.

**Negotiations** (Schedule 7 Paragraph 7) - where personal data consist of records of the intentions of the data controller in relation to any negotiations with the data subject to the extent that disclosure would be likely to prejudice those negotiations.

**Examination Marks** (Schedule 7 Paragraph 8) - students cannot find out their exam mark before the results day by making a subject access request. Exam marks are exempt from the usual 40 day timescale, but data controllers must disclose this data either five months from the day on which they receive the request or 40 days from the announcement of the exam results, whichever is earlier.

**Examination Scripts** (Schedule 7 Paragraph 9) - these are exempt from subject access, but examiners' comments are not exempt and students have a right of access to these.

**Self-incrimination** (Schedule 7 Paragraph 11) - where complying with a subject access request would reveal evidence of the commission of any offence, other than an offence under the DPA 98, exposing them to proceedings for that offence.

**Third party data**

Some data, especially e-mails, may contain personal data relating to third parties. When responding to subject access requests, the University will need to consider the rights of third parties and ensure that they are not compromised. This may mean that consent from third parties to release data is sought or that relevant sections of documents are deleted. The University will also consider Article 8 of the Human Rights Convention which specifies that 'everyone has the right to respect for his private and family life, his home and his correspondence.' E-mails written in a private rather than an official capacity are therefore unlikely to be released without the consent of the third party.