RM Framework Guidance Document: Data Protection in the Workplace

1. Aim

Staff members who process personal data about students, staff, applicants, alumni or any other individual have particular responsibilities under the University's Data Protection Policy. The aim of this guidance is to highlight these responsibilities and to provide practical advice to some common Data Protection scenarios.

2. Background

The Data Protection Act 1998 controls the way personal data can be handled and provides legal rights to individuals who have information stored about them. As a Data Controller, the University has legal responsibilities to manage personal information in accordance with the Act, and in turn individual members of staff have responsibility for appropriate handling of data. Staff training and awareness about Data Protection ensures that we have in place organisational measures to make sure all our staff are processing personal data appropriately; this in turn helps to prevent data breaches from occurring through negligence.

3. What is Personal Data?

If you hold information about individuals either on computer or in paper records you may be holding 'personal data'. Personal data is data that:

- Identifies an individual, either on its own or combined with other information within the University
- Includes opinions in regards to that individual
- Includes information which informs or influences decisions affecting an individual
- Conveys biographical information about the person – the fact that an individual attended the meeting will be personal data about that person.

4. General Staff guidance

These top ten tips are not exhaustive but provide a basic overview of some important aspects of Data Protection you should be aware of:

1. **Attend basic training.** Make sure you understand what your responsibilities are. Data Protection courses are run monthly at the University and compulsory podcasts have been produced for all staff
2. **Don't disclose personal data** to any person or third party unless you have the permission from that individual (or a legitimate reason)
3. **Use privacy statements** if you ever collect personal data for any legitimate reason. Make sure you explain why you need it, what you are going to do with it and how long you intend to keep it
4. **Refer to the Tri-Campus Data Sharing Agreement** if you need send personal data to our overseas campuses
5. **Report all personal data breaches** straight away, early identification may help to recover or contain the data breach and prevent further damage
6. **Requests for an individual's own personal data are called Subject Access Requests.** If it is not data you would routinely disclose to an individual in the course of your work, direct the individual to the Governance Team
7. **Confirm a caller's identification** before you disclose any personal details to any individual. Ask basic security questions to satisfy yourself you are speaking to the individual they claim they are
8. **Don't put personal information in emails if you don't want it disclosed**. Emails are not secure and can be disclosed under Subject Access Requests
9. **Destroy means destroy.** Always shred paper records containing personal information
10. **Keep personal data securely.** If you have personal data in your records make sure you keep them securely and delete them as soon as they are no longer needed

5. Staff Responsibilities

In accordance with the University's Data Protection Policy, staff members must ensure that:

- all **personal data is kept securely**;
- **no personal data is disclosed** either verbally or in writing accidentally or otherwise, to any unauthorised third party;
- personal data is **kept and destroyed in accordance with the University's retention schedule**;
- any queries regarding data protection, including **subject access requests and complaints, are promptly directed to the Governance Team;**
- any data protection **breaches are swiftly brought to the attention of the Governance Team** and that they support the Governance Team in resolving breaches;
- where there is uncertainty around a Data Protection matter **advice is sought from the Governance Team.**

6. Common Data Protection Situations

The following are common situations we might experience in the workplace. The notes that follow explain what you should do in each scenario. If you are ever in doubt, contact the Governance Team.

i. I am called by a student wanting to discuss their personal data
ii. I am contacted by a parent to discuss their child's progress
iii. I have accidently disclosed some personal information to someone I shouldn't have
iv. I want to share personal information with a third party
v. I want to email a colleague about a personal issue I have about another individual
vi. A student has asked me for a copy of their personal information
vii. I need to send some personal data to our overseas campuses
viii. I have been contacted by the police to confirm some personal details about a student
ix. I've received a complaint from a student about how we have used their personal data
x. I'm a committee secretary, how should I document personal information within minutes

i. I am called by a student wanting to discuss their personal data

Under the Data Protection Act, the University is obliged to take reasonable steps to confirm the identity of a telephone caller before proceeding with a call involving the disclosure of personal data. Always satisfy yourself that the person you are speaking to is who they say they are. It is good practice to always ask some basic security questions such as, date of birth, home address plus any other information that only that student would be able to answer. If you have any doubts use your discretion and let the student know you will call them back on their registered phone number.

ii. I am contacted by a parent to discuss their child's progress

Parents, other relatives and third parties often contact the University to request personal data about students at the University (for instance, it is very common for parents, particularly those who are contributing to tuition fees, to ask for information about the academic progress of their son or daughter, or to try and find out where they are since they have not been in touch). Unfortunately, the University is not able to disclose this sort of personal data (even to parents) other than in the most exceptional of circumstances.

Has the student given you their explicit permission to talk to the individual you are speaking to? If you do not have prior consent you should not even confirm that the individual is even a student at the University of Nottingham. Student status is personal information and disclosure could be a data protection breach.

Example:

Caller: *"I'd like to talk to you about my son who is studying at your school, I'm worried that he might be having a few problems….."*

***Response**: "I'm sorry but the University has a policy not to discuss personal data with any other person other than the data subject unless we have signed prior consent from the individual concerned"*

***Caller**: "Yes, I am sure he has given consent….he name is…."*

You can find the student but there is no evidence of consent.

***Response**: "I am sorry but you will have to speak to your son. Under the Data Protection Act, I am unable to confirm or deny that we have any student of that name studying here. I would recommend that you contact your son about this as I am unable to discuss this further with you".*

Contact the student concerned and let them know, they may well provide you with the consent for next time. If you have consent from the student to speak to a third party, make sure you ask that individual enough security questions to satisfy yourself that they are that named person. If you are in any doubt about the callers' identity, do not continue with the conversation. Contact the student and ask them to confirm consent verbally. Information discussed should be limited to the topic agreed with the data subject.

iii. I have accidently disclosed some personal information to someone I shouldn't have

Where a Data Protection breach occurs, or is suspected to have occurred, the Governance Team should be notified as soon as possible. The Governance Team will work alongside the relevant department(s) to:

- minimise the damage;
- assess the extent of the damage and determine whether the ICO should be notified;
- notify individuals affected as appropriate;
- ascertain how the breach occurred and, if appropriate, determine how to prevent or minimise future breaches.

iv. I want to share personal information to a third party

The University's Data Protection Statement lists all third parties whom we routinely share students' personal data with. These are legitimate circumstances for data sharing that we notify students about.

If you intend to share personal data with a third party not listed on the Data Protection Statement please contact the Governance Team to discuss this. There are legitimate reasons for sharing information to other third parties but you will need to ensure this is in accordance with the Act. You may need to get consent, write a privacy statement and sign a data sharing policy.

v. I want to email a colleague about a personal issue I have about another individual

An individual has a right to a copy of their personal data on written request. An opinion about someone is actually their personal data under the Act and could be disclosed. Unless you wish to make an official statement, don't use email to discuss personal or private matters that involve personal data. Don't put anything in writing that you wouldn't be prepared for that individual to see. Emails should state facts and not include subjective opinions. Emails may be disclosed under a subject access request and to conceal or destroy data with the intention of preventing access is a criminal offence.

vi. A student has asked me for a copy of their personal information

Unless you would routinely provide an individual with a copy of their personal data on request, a request for personal information should be treated as a Subject Access Request. Subject Access Requests (or SARs) are requests for a copy of an individual's personal data. This would not necessarily be an entire document, only the information relating to the individual.

All SARs are handled by the Governance Team within 40 calendar days. Please ensure you notify us as soon if you receive one so that we can respond within this designated timeframe.

Subject Access Requests are only valid if they are made in writing

vii. I need to send some personal data to our overseas campuses

The Tri-Campus Data Transfer Policy explains conditions for how personal data may be transferred.

Security is of the utmost importance when sending data outside of the EEA. Please contact the Governance Team if you have any questions.

viii. I have been contacted by the police to confirm some personal details about a student

The University sometimes receives requests from the police for personal information about students. Most Police Forces will have their own request form which should always include a statement confirming that the information requested is required for the purposes covered in Section 29 of the Data Protection Act, a brief outline of the nature of the investigation, the student's role in that investigation, and the signature of the investigating officer. Do not disclose information to the police over the phone. Check with the Governance team first that the information can be released.

ix. I've received a complaint from a student about how we have used their personal data

All complaints relating to the handling of personal data must be forwarded to the Governance Team who will assist in investigating the matter appropriately. If a data breach has occurred it is important that we can respond in accordance with our data breach reporting policy.

x. I'm a committee secretary, how should I document personal information within minutes

There are two types of personal data contained within minutes; information about those individuals attending the meeting and information about those discussed in the meeting.

It is generally good practice to avoid attributing individual comments to a named attendee at the meeting. A committee works as a collective and singling out individuals is often unnecessary. If someone shares advice or information in their professional role then it is appropriate to name them or give their job title.

If individuals are discussed in a meeting, it is likely that they will need referencing in the minutes either by name or by an ID number. Bear in mind that the individual concerned has the right to see what is written about them if they so request. No individual has the right to see information about another individual contained within the same set of minutes, and it may be necessary to redact information before it is disclosed.

Minutes that contain personal data should only be shared with those who need to have access.

7. Useful Links

All staff are advised to read the full Data Protection Policy:

http://www.nottingham.ac.uk/governance/records-and-information-management/data-protection/data-protection-policy.aspx

The following Data Protection podcast is mandatory for all staff:

http://www.nottingham.ac.uk/legalservices/podbriefings/data-protection.aspx

Data Protection Training is now available monthly as a University short course:

https://training.nottingham.ac.uk/cbs-notts/Guests/GuestCourse.aspx?CourseRef=EDPS

The Information Commissioner's Webpages contain useful guidance materials and best practice examples:

https://ico.org.uk/