DATA PROTECTION: FAQs

1. Can I share personal data within the University?

Where there is a strictly need to know reason for disclosing personal data about a student or staff member and there is a reasonable expectation by that individual that their data may be disclosed, then an appropriate sharing of data is permitted. However, you must then consider the method by which you do this and to whom you disclose the data. Any emails should be marked as confidential to alert the recipient and discourage any inappropriate forwarding or copying in to a response.

Where the data is considered to be sensitive e.g. it concerns physical or mental health or a disability, then the written consent of the individual is required before any such data can be shared. Further information on data sharing is available in sections 8.1 and 8.2 of the Code of Practice

2. I've received a request from a parent. What can I tell them?

Whilst we may have every sympathy with the parent who may be funding their son or daughter's education and consider that they are sponsoring their education, we are unable to disclose any personal data about their son or daughter without the individual's consent, which should be in writing. This applies to all enquiries about University students irrespective of whether they are under the age of 18.

However, this does not mean that you are unable to respond at all to the parent e.g. with details of our policies and procedures, term dates or how a student may make a complaint. In certain cases it may be acceptable to take a message and pass this on if subsequent checks confirm that the individual is a student at the University. But in doing so you must be careful not to disclose to the enquirer whether or not the individual is a student.

3. I've received a request for student data from a sponsor. What do I do?

Some of our students have a formal financial sponsorship arrangement with a company, prospective employer or their home country's Embassy, who may then request details of their sponsored student's attendance and academic progress. You should check with Finance whether there is a formal sponsorship agreement in place for the student. If you're in any doubt then you should contact the student direct and ask them to confirm this and seek their consent to disclose their data.

Once you have done your checks or received consent, you should only provide basic limited information about a student's academic progress and attendance; anything else will be regarded as excessive.

If attendance has been interrupted or affected e.g. due to ill health, since this is sensitive personal data we must have the written consent of the student to disclose this and the reasons for the absence to their sponsor.

Further information and guidance on disclosures and the appropriate secure method of doing this are in sections 8.5 and 8.6 of the Code of Practice.

4. A police officer is asking me for data about a student. What should I do?

We are not required to provide personal data to a police officer, or any other officer who is pursuing an investigation for the purposes of criminal or civil proceedings. There is a prescribed University procedure for the handling of any such requests. No disclosures should be made before referring the enquiry to Governance Services, where they will be considered and responded to as appropriate. Further details are in sections 8.5 and 8.6 of the Code of Practice.

5. I've been asked by an employer to verify a student's award. Can I do that?

The University will often be contacted by employment agencies, prospective employers and other third parties to verify details about a student or to ask if a member of staff is employed at the University. Such requests for information should be treated as a request under the Freedom of Information (Scotland) Act 2002 and the University will need to consider whether an exemption applies where it relates to personal data. Full guidance on what to do is in section 8.10 of the Code of Practice.

Where a student or member of staff claims that they have attained an award and this is proved to be false you should consult the guidance in section 8.11 of the Code of Practice.

6. ENSA / ENSA Advice have phoned me and asked me to confirm some student data. Can I do this?

The University works closely with Edinburgh Napier Students' Association (ENSA) and ENSA Advice (formerly the Independent Student Advice Service) for the benefit of students but staff must remember that ENSA and ISAS are independent of the University. This means that before we disclose any data to them we must be satisfied that the student has given their consent for us to do so. Whilst we would not want to create or add to any academic or pastoral difficulties a student may be experiencing, if you are in any doubt then ask to see a copy of the student's disclosure form or contact the student to seek their consent and/or send them the requested data, which they can then forward as appropriate.

7. How do I find out what personal data the University holds about me?

Under the Data Protection Act 1998, you have a right of access to your personal data. The University has a prescribed procedure for this, information on which is in the guidance on Access to Personal Information . However, if you would like to see only one or two documents which you believe contain your personal data then you should contact the Information Governance Manager to discuss this.

8. I have to write a reference. What do I need to consider?

University staff are routinely asked to provide internal and external references for students and other staff. There are important legal and other considerations to note in

doing so and The Guidance Note on References should be consulted before any reference is provided on behalf of the University

9. Can I see a reference that has been written about me?

This will depend on who wrote the reference. If a member of University staff has written a reference about you then this is generally exempt from your right of access under the Data Protection Act 1998. However, if a third party has written a reference which has been received by the University then this is not exempt, but consideration must be given to the data privacy rights of the referee. Further guidance on this is in section 19 of the Code of Practice.

10. I have to transfer a batch of student records to a third party. How should I do this?

Before you send any personal data out of the University whether electronically or in hard copy, you must ensure that you have the relevant University authority to do this i.e. permission from your line manager or you are satisfied that the transfer is in pursuance of an agreement or is required by law. You must then ensure that the data is transferred as securely as possible having considered the level of sensitivity and volume of the data to be sent. You must not:

- Assume that documents transferred by electronic means e.g. email, web transfers, File Transfer Protocol are secure
- Send any material containing sensitive personal data, or data that if it should be lost is likely to cause damage or distress to the subjects unless it has been encrypted
- Download personal data onto physical devices e.g. USB memory sticks, CDs or DVDs unless absolutely necessary; you must then ensure such devices are appropriately encrypted
- Send hardcopy data in the mail unless it's marked strictly private and confidential, is addressed to a named individual and sent recorded delivery

More guidance is in s.7.5 of the Code of Practice

11. I've been told I need to encrypt personal/ confidential data I am sending out of the University. How do I do this?

Information Services publish guidance on the encryption of confidential or sensitive data using TrueCrypt and on email encryption.

12. I want to set up a social networking site for students on my course. What do I need to think about before I do this?

You should check first with Information Services whether this can be hosted internally. If for good reason you decide that what they can offer does not meet your requirements then you need to be aware that there are significant data protection and legal issues which will be relevant if you go to an external service provider. Consult the guidance on Web 2.0 services for further information and in particular the Guidance for Staff .

13. I'm the personal tutor for a student with a disability. As I'd like to help support their academic studies what information can I pass on to others in my School?

As physical or mental health matters and conditions are sensitive personal data, you must take extra care in the handling of any information which relates to such matters. Normally, you must not disclose any information to any other individuals without the express written consent of the subject, even where this may adversely affect their studies. Further guidance is in section 12 of the Code of Practice.

14. I've moved offices and don't have enough space for all my records. Can I put them out for the cleaners in a black bin bag?

Under the Data Protection Act, you should only keep records which contain personal data "for as long as is necessary". How long you should keep such data will depend on what it is and whether there are statutory or professional requirements or best practice considerations for retaining it. The University is developing records retention schedules which you should consult before you dispose of any records. If there isn't a schedule for your area then you should consult section 20 of the Code of Practice or contact Governance Services

Once you've decided that you can dispose of records which contain personal or confidential data you must ensure this is done securely by placing them in a console bin provided by the University's contractors for the disposal of confidential waste or failing that, by shredding the records. You must not put these records in either the normal waste disposal or recycling bins. Further guidance is available in section 7.9 of the Code of Practice.

15. I work from home. What do I need to consider?

All University staff who work from home, either on an occasional or a regular basis, must be aware of their obligations under the DPA 1998, the Freedom of Information (Scotland) Act 2002 and the University's Information Security Policies. Security of personal data is paramount when any personal data is accessed remotely or physically removed from University premises and must be ensured whether you are doing administrative, research, academic or other teaching-related work. Key points are:

- If you have to take manual or electronic personal data home, you must ensure you use all appropriate security precautions to guard against inappropriate or unauthorised access

- If you download personal information to a removable device e.g. USB stick, CD, DVD or to a University laptop you must encrypt the device or laptop

- Don't leave personal information unattended at home, in cars or briefcases, locked or unlocked

- You are strongly advised to set up a virtual private network (VPN). You must also keep back-ups of information and consider the most secure way to do this

- You must return all personal data to the University for secure disposal

Section 7.8 of the Code of Practice gives guidance and further links on what you should do to ensure there are no security breaches.

Note that the University can be fined up to £500K for serious breaches of data security.

IT publish guidance on Remote Access to the Network which explains how to install and use a virtual private network.

HR's Homeworking Policy, available from the HR Documents intranet page, addresses the relevant issues in section 9 and Appendix 4.

16. I've had an email from a student asking me to give them copies of the information the University holds about them. What should I do?

Where an individual is seeking their personal data, this is called making a subject access request and must be dealt with under the Data Protection Act 1998. You should respond by sending the student a link to the University's guidance on Access to Personal Information which includes a form and information about the process, the fee, verification of identity which may be required and the timescale of 40 calendar days for our response. The form is intended to assist the individual and the University in specifying the information being sought and where it may be held, but completion of the form is not compulsory as long as the request has been made in writing, the fee has been paid and identity has been verified where necessary. If the student is looking for one or two specific documents rather than everything the University holds about them, then you should discuss this with your line manager or the Information Governance Manager before invoking the formal process.

If they (or any third party) are looking for information about someone else this should be treated as a request under the Freedom of Information (Scotland) Act 2002 and submitted to foi@napier.ac.uk

17. I've been asked to delete electronic records containing personal data. What should I consider?

The Data Protection Act 1998 does not define 'delete' or 'deletion' but a plain English interpretation implies 'destruction'. As with manual data the University holds, it's important to ensure that electronic data is securely disposed of at the appropriate time to comply with the data protection principle that states that personal data shall not be kept for longer than is necessary. You should consult your area's records retention schedule (if one has been developed) to check whether the data is due to be deleted and if so whether this is to be done permanently or is to be preserved as archival information. If your area does not have a schedule in place you should consult s.20 of the Data Protection Code of Practice or contact the Governance Adviser (Records Management).

The UK Information Commissioner oversees compliance with the Data Protection Act 1998 and has published guidance for organisations on Deleting Personal Data.

You should be aware that the contents of an email or email folder are not to be regarded as deleted merely because you have moved it/them to your 'Deleted Items' folder. You should ensure you delete relevant records permanently from this folder and similarly, you should empty your desktop 'Recycle Bin' for other electronic records which you've deleted.

18. I would like to delete personal data I've stored on my home computer and/or on a PDA/DVD/CD. How should I do this?

The UK Information Commissioner, who oversees compliance with the Data Protection Act 1998, has issued guidance for individuals on Deleting your data from computers, laptops and other devices

19. I want to use a cloud computing service for personal data. What do I need to know?

Cloud computing services provide data processing and storage facilities which are external to the University. Some of these services may be hosted overseas in countries which do not have the same privacy protections required by the Data Protection Act 1998. Staff must be aware therefore that breaches of the Act could arise from using these services, unless there is a robust data sharing agreement in place.

The University already publishes comprehensive guidance on the use of Cloud Computing Services which must be consulted and also this guidance on Using Cloud Computing Services for events management or advising students about advertised Cloud Services.

20. I have received a Court Order. What do I do with it?

The University receives a number of court orders in the course of a year, many of which are for the production of documents the University may hold within 7 days of the order being served. The purpose of this guidance is to highlight the key points which all University staff must be aware of in ensuring a Court Order is dealt with timeously and correctly.

Governance Services
Updated August 2017