



Data Protection

For Staff & Students



What is Personal Data (Information)?

Personal data is information that relates to a living identifiable individual e.g. name and date of birth or matriculation number and course. Personal data may be held in many formats, including emails, electronic documents, on social media, manual filing systems, CCTV, photographs and handwritten notes e.g. of meetings and phone conversations.

Certain types of information are classed as sensitive personal data e.g. where it's about physical or mental illness, faith or religious beliefs, criminal convictions and trade union membership. This information should only be shared with informed written consent.

Security of Personal Information

Staff and students processing personal data on behalf of the University must ensure that manual and electronic data are kept secure at all times, in accordance with the University's Information and Manual and Physical Data Security policies. This includes locking away all manual data when not in use and restricting access to electronic data to the necessary personnel.

DO:

- Anonymise personal data wherever possible - take out anything which could directly/indirectly identify a person
- Choose a strong password that has a mix of at least 8 characters, keep it secure and don't share it
- Use encryption on emails and portable devices and access permissions on shared folders/sites to prevent unauthorised access
- Mark letters 'strictly private and confidential' and send to a named individual
- Always consider the most appropriate secure method of sending manual or electronic personal data
- Use MyDrive or a Virtual Private Network when working from home or remotely

DON'T:

- Disclose personal data without consent or where this isn't permitted by law
- Take or send physical devices containing personal data out of the University unless they've been encrypted
- Assume that email is private or a secure method of communication
- Email sensitive personal data externally unless it has been encrypted
- Allow inappropriate access to personal data either at work or home
- Leave personal information in manual or electronic format unattended in cars or briefcases even when locked

Further information and guidance on data security is available from the Governance Services intranet site at:

staff.napier.ac.uk/personaldata

or in the University's Information Security Policy at: staff.napier.ac.uk/infosecurity



Confidentiality

All staff and students processing personal data must keep this information confidential at all times. Individuals should not be discussed by name or identifiable title in public places and personal data must not be visible to unauthorised third parties, on or off University premises. Personal information should only be shared internally, where necessary and in an appropriate manner, to support the ongoing business of the University.

Use of personal data

The purposes for which the University uses your personal data are explained in these statements for staff and students:
staff.napier.ac.uk/dpstatements



Release of Personal Information

There are some circumstances in which the Act allows the University to release your information to a third party. These include where:

- you have given consent for your personal information to be provided to named third parties
- there is a statutory or legal requirement to do so
- failure to disclose the personal information would endanger you or others or not be in your best interests

If you would like further information or guidance on the release of your personal data please contact the Senior Governance Officer (Data Protection & Legal).

Overseas transfer of personal data

Personal data may not be transferred to non EEA countries unless certain conditions have been met. This includes the use of cloud computing services hosted overseas. Guidance on this is available at:
staff.napier.ac.uk/datatransfer

Complying with the Act

Compliance is the responsibility of all staff and students. Any deliberate or reckless breach of the Act and its requirements may lead to disciplinary action being taken. In addition, the UK Information Commissioner has the power to fine the University up to £500,000 for any serious breaches of the Act or to take other action.

Student Permission to Disclose

There are forms available on the Governance Services site for use where student consent is needed for a disclosure of personal data.

At matriculation students are given the option of having their data transferred to Napier Students' Association and to taking part in some surveys.

Students may change their data protection consent status at any time by going to Personal Record on the student portal, visiting www.napier.ac.uk/nimweb or emailing records@napier.ac.uk

Graduation Ceremonies

The University's Graduation Ceremonies are regarded as public events. Students who are intending to graduate or may be eligible for an award should read the important information about the use of their personal data for the purposes of these events at:
www.napier.ac.uk/graduations

CCTV

CCTV is covered by the requirements of the Act. The University uses CCTV at its main campuses for the purposes of public safety and security and the prevention and detection of crime. If you would like further information on CCTV and your rights under the Act, please contact the University's Head of Campus Services or email SecurityControl@napier.ac.uk

Rights under the Act

The Act gives you rights e.g. to:

- be told how we will use your data
- correct your data if it's wrong
- object to processing which may cause you harm or distress
- prevent your data being processed for direct marketing purposes
- have access to your personal data

You can ask the University for copies of records containing your personal data by making a Subject Access Request. The University has 40 calendar days to respond to your request and there is a fee of £10. Information on how to go about this, together with the University's form and who to contact with any enquiries, is available at: staff.napier.ac.uk/accessyourinfo

Other information and guidance on your rights is available from the UK Information Commissioner's website at: <http://ico.org.uk>

Retention of data

Personal Information about staff and students will be kept in accordance with the University's records retention schedules. Any enquiries about the retention of records should be referred to the Senior Governance Officer (Records Manager) or Senior Governance Officer (Data Protection & Legal).

Disposal of personal data

After consulting the relevant retention schedule, manual records should be carefully disposed of by placing them in dedicated console bins. Electronic data must be overwritten or deleted and then removed from desktop recycling bins and deleted emails should be removed from the deleted items folder. Physical electronic devices e.g. CDs, DVDs, Blackberrys, PDAs, Tablets, memory sticks containing personal data must be disposed of in accordance with University policy. Further information is available in the University's Information Security Policy and also in the Guidance on the Safe Disposal of Confidential Waste at: staff.napier.ac.uk/datadestruction



How does the Data Protection Act 1998 (DPA) fit with the Freedom of Information (Scotland) Act 2002 (FOISA)?

Both Acts govern information held by the University. Whilst the DPA relates to personal information we hold about an individual and can only be requested by that individual, the FOISA is concerned with recorded information we hold as a public authority and can be requested by anyone. Although these two acts have quite different purposes there is some interaction between them. Further information is available at: staff.napier.ac.uk/dpfoi



Data Protection Act at Edinburgh Napier University

This leaflet is designed to give you some information about the Data Protection Act 1998 (the Act) and how it may affect you.

The purpose of the Act is to protect your privacy and give you certain rights to ensure that your personal data (information) will be processed in accordance with the requirements of the Act. This includes how your data is collected, held, used and destroyed.

The Act also imposes obligations on staff and students who handle personal data to do so in accordance with the Act, including making sure data is kept securely.

Further Information

Data Protection Act (DPA)

Further information and guidance is provided on the Governance Services intranet site at **staff.napier.ac.uk/dataprotection**



If you have any questions on this Act and the use of your personal information or want to know more about your rights please contact:

Governance Services

Email: **dataprotection@napier.ac.uk**

The UK Information Commissioner is responsible for ensuring compliance with the Data Protection Act 1998 throughout the United Kingdom. Further information is available from **www.ico.org.uk**

Freedom of Information (FOI)

Please visit the University's FOI website at **www.napier.ac.uk/foi**

or email the Senior Governance Officer (Records Manager) at **foi@napier.ac.uk**

staff.napier.ac.uk/governance

