

DATA PROTECTION FACTSHEET FOR STUDENTS

KEY THINGS YOU SHOULD KNOW

- 1 Edinburgh Napier University will only disclose your information if we have your consent, we are required to by law or it's allowed by Data Protection Legislation
- 2 You need to ensure that the personal information you give us is accurate and kept up to date
- 3 Lock your computer or log off completely whenever you leave your workstation - do not expect it to lock on its own – and remember to remove any USB sticks
- 4 Don't leave your laptop, iPad or other physical devices unattended at any time in the University or otherwise in a public place
- 5 You have rights under Data Protection Legislation to access your personal data, prevent direct marketing & automated decision making and to have your personal information corrected
- 6 If you're processing personal data about others as a research or employed student or a student representative, you must comply with the Act and the University's [Data Protection Code of Practice](#)

TOP TIPS FROM THE [UK INFORMATION COMMISSIONER](#)

- Treat your personal data as 'confidential' – don't give it away easily
- Always be wary of those asking for your personal information. Are they genuine? How will they use it? Will it be passed on to others?
- Sign up with the Telephone Preference Service to prevent unsolicited direct marketing calls
- Know where your personal documents are (passports, driving licence, birth certificate etc.) and keep them safe
- If you receive letters, emails, texts messages or telephone calls asking for your information, avoid replying unless you know they are genuine
- Always read the small print carefully. You must give permission for your details to be passed on to other organisations or used for marketing purposes, and equally, you can refuse
- Never disclose or write down personal passwords or PIN numbers
- Destroy your personal documents, (such as bank statements, utility bills, debit or credit card transaction receipts etc.) when you no longer need them, so that nothing can be obtained by fraudsters showing your name, address or other details
- Always check your bank / credit card statements for payments you don't recognise
- Just say no – you have the legal right to ask a particular company to stop contacting you and they have an obligation to mark your telephone number as one they cannot call