Edinburgh Napier University
Security of Personal Information: Staff Checklist

NB: THE UNIVERSITY COULD BE FINED A MAXIMUM €20M FOR SERIOUS BREACHES OF DATA SECURITY

This checklist has been adapted from guidance issued by the UK Information Commissioner for quick reference purposes; further detailed information and guidance is provided at:
http://staff.napier.ac.uk/services/secretary/governance/DataProtection/Pages/SecurityofPersonalData.aspx
and: staff.napier.ac.uk/services/cit/infosecurity/Pages/InformationSecurity.aspx

1. Keeping personal information secure

- Keep passwords secure – choose one that isn't easy to guess, change regularly and don't share it; lock /log off computers when away from your desk
- prevent virus attacks by taking care when opening emails & attachments or visiting new websites
- ensure that computer screens are positioned appropriately in open plan offices and away from windows to prevent accidental disclosures of personal information; do not process personal or sensitive data in public places e.g. buses, trains, planes, or University canteens/cafes
- always use encryption if personal information must be taken out of the office e.g. on a laptop, PDA, iPad, memory stick, CD or DVD; take particular care with all physical devices to prevent inadvertent loss or theft
- if you must take manual or electronic personal data home, you must ensure you use all appropriate security precautions to guard against inappropriate/unauthorised access; do not leave personal information unattended at home or in cars or briefcases (locked or unlocked)
- If you work from home you are strongly advised to set up a VPN to do so; you must keep back-ups of information and consider the most secure method of doing this
- do not assume that email is a private or secure medium; consider whether personal data, particularly sensitive personal data, needs to be emailed internally and in what format. Do not forward emails inappropriately and anonymise where appropriate. See 3 below for external emails
- confidential waste, in paper and other formats, must be disposed of securely in dedicated console bins provided by the University; confidential waste sacks must not be used. If working from home you must return all personal data to the University for secure disposal
- work on a 'clear desk' basis; store hard copy personal information securely when not being used
- sign your visitors in and out at your campus reception desk and ensure they're accompanied in areas normally restricted to staff

2. Disclosing personal information

- do not release personal data without consent or where this isn't permitted under the legislation. If in any doubt seek advice from your line manager or Governance Services
- all requests for disclosure should normally be made in writing on official headed notepaper and addressed to a named individual in the University
- where a disclosure is appropriate, do not provide irrelevant or unnecessary information
- be aware of third parties who will try to obtain personal information by phone. Prevent an unauthorised disclosure by checking out the identity of the caller before deciding what personal information if any is appropriate to give out. If in doubt take a number and get advice before calling them back via their main switchboard; similar checks should be performed when making outgoing calls. Follow up with written confirmation where necessary

3. Sending personal data

- consider whether you are permitted to email personal data; anonymise data wherever possible
- send letters marked strictly private & confidential to a named person; consider recorded delivery
- if you have to fax personal data, extreme care must be taken to check the correct number and recipient; if in any doubt don't do it
- physical devices containing personal data must be encrypted before being sent; then consider the most appropriate secure method, e.g. hand delivery, registered delivery or courier
- note that sensitive personal data must never be emailed externally unless encrypted