



THE UNIVERSITY *of* EDINBURGH

DIVISION OF CLINICAL NEUROSCIENCES

Storage and Use of Electronic Personal Data

Information for Staff on the Storage and Use of Electronic Personal Data

This guidance highlights the general issues to consider when storing and using information about living, identifiable individuals in an electronic format to ensure that personal information is kept secure and the University complies with its obligations under the Data Protection Act 1998. In some circumstances you will need to take additional measures; to see the full range of guidance available, visit the University's data protection home page. This document was written by Jenny Middleton and Susan Graham of the University Records Management Office and is reproduced with their permission.

Who is this guidance for?

This guidance is for all members of staff who store personal information in an electronic format. This includes word processed documents, spreadsheets, databases and e-mails, all of which can be found on and accessed via various devices such as your desktop, laptop PCs, PDAs, mobile telephones, USB memory devices, CDs and DVDs.

The document includes tips for users of Microsoft Windows. Over time, information will be added about other environments commonly in use around the University.

Why should I be concerned about this?

The Data Protection Act 1998 applies to all "personal data" about a living, identifiable individual. It sets out how we should use this information. Failure to comply with this Act could expose the University of Edinburgh and individual to legal proceedings or reputational damage.

The definition of personal data is highly complex. For day-to-day purposes it is best to assume that *all information about a living, identifiable individual is personal data*. Attached is a brief guide to determine what exactly personal data is. For a fuller explanation, please visit the University Records Management website

Dos and Don'ts

Do:

- ✓ Anonymise personal information whenever possible.
- ✓ Practice good IT security. Please refer to the University's Computing Regulations and the University's IT security policy for more information.
- ✓ Use encryption, access permissions and other features to restrict access to personal information to staff who need to see it to do their job.
- ✓ Take particular care when transporting personal information to different locations (including passing data to other organisations). Encrypt the data and ensure that physical devices cannot be accidentally lost, for example, by using special delivery post or by not leaving the device unattended.
- ✓ Take appropriate security precautions if you take any information about people home with you. Make sure it cannot be accessed by thieves or accidentally viewed by visitors or family members. For further information see the guidance on home working.
- ✓ Choose a password that is not easy to guess.

Last updated February 2011

The University of Edinburgh is a charitable body, registered in Scotland, with registration number SC005336.

- ✓ Site PCs where the screen cannot be seen by unauthorised staff or the public.
- ✓ Lock your computer, if possible, if you are leaving your desk for more than 5 minutes.
- ✓ Delete personal data as soon as it is no longer required.
- ✓ Ensure that your deleted items are actually deleted – simply deleting items does not always remove them completely from your computer. For example, in Microsoft Outlook when you delete e-mails they are moved to and stored in your 'deleted items' folder and you must also delete them from here. Similarly in Windows when you delete items from your computer they will often be sent to the 'recycle bin' on your desktop, from where you must delete them again.
- ✓ Take particular care when disposing of or selling a PC or any other device that potentially holds personal data – ensure that all personal information has been deleted.
- ✓ Use the network in preference to your hard drive whenever possible, this makes back ups, deletion and legislative requirements easier to manage.
- ✓ Take action if you suspect unauthorised staff have accessed personal information.
- ✓ Be careful when embedding documents - when you embed a document it is possible for the reader to access the entire document and not just the information on display.
- ✓ Ask the IT support team for advice on making your computer and your information secure.

Don't:

- ✗ Assume that information has been anonymised just because you have removed names – codes may still link the information to particular individuals, or they could still be identified from the data that remains, for example a combination of department, ages and gender.
 - ✗ Leave information on the screen when you are not there – have your screensaver set to activate quickly if you leave your computer unattended.
 - ✗ Assume that e-mail is a private or secure form of communication.
 - ✗ Share your password.
 - ✗ Write your password down. If you must write it down then don't store it in an easily accessible place
 - ✗ Send someone's username and password in the same e-mail or document, send them under separate cover.
-