Email and personal data: preventing unauthorised disclosure

The University has a responsibility under the Data Protection Act 1998 to ensure that personal information or data is only disclosed to those who are authorised to receive it.

The Information Commissioner now has powers to impose fines of up to £500,000 on organisations responsible for a 'significant' data loss which results in the actual or potential unauthorised disclosure of personal data. Accidental disclosure through sending emails to unauthorised people is a particular problem and has recently resulted in the Information Commissioner imposing fines of up to £140,000.

The guidance has been prepared to assist all staff responsible for personal data in ensuring that the risks of unauthorised disclosure of such data are minimised, and should be read in association with the IT Computing Regulations available at: http://its.southwales.ac.uk/documents/download/4/

- Review the classes of personal data you hold and the means of distribution you use. Identify any highly sensitive or confidential data. This will include 'sensitive personal data' as defined in the University's Data Protection statement (available at http://uso.southwales.ac.uk/ig/dp/), personal financial data, and any data to which the University has applied a higher security category.

- Where possible, avoid the use of email to distribute personal data. Consider authorised access to SharePoint as an alternative.

- Encrypt all documents containing highly sensitive or confidential data by setting a password. This facility is readily available in recent versions of Microsoft Word, Excel and PowerPoint – see 'Technical arrangements for encryption' below for more details.

- Do NOT use your University password to encrypt the document.

- Make sure you remember the password as encrypted documents cannot be recovered without it.

- Never store documents containing personal data in the same folder as documents which can be freely distributed. E.g. do not place completed forms or spreadsheets summarising completed forms in the same folder as blank forms. Use distinctive filenames to make it easy to distinguish between the two categories of document.

- If email is the only feasible means of distributing personal data to authorised users:

  - Check regularly that mailing lists contain only those currently authorised to receive the document and that email addresses are accurate and up to date – remember that just one character difference in an email address could result in your message going to the wrong person.

- Never include highly sensitive or confidential data in the body of the email. Such data should only be included in an encrypted attachment.

- Check carefully that the attachment contains only the information you need to distribute. E.g. on spreadsheets check for 'hidden' columns and additional tabs that may contain information that should not be distributed.

- Never distribute encrypted documents and passwords in the same email; it is preferable to exchange passwords face to face or by telephone.

Please contact the LCSS Information Governance team by emailing dataprotection@southwales.ac.uk if you need any assistance in following these guidelines.

Technical arrangements for encryption

The encryption of Microsoft Office documents via a password is acceptable if:

- The version of Office being used is Office 2007 SP2 or greater. That is, make sure the latest service packs for Office 2007 and 2010 are installed.
- Documents are saved as .docx, .xlsx, .pptx. Don't save them as .doc, .xls etc.
- A strong password is used, in keeping with our standard password advice (http://its.southwales.ac.uk/securing-account/).

Users with Office 2003 can read a document that has been encrypted with Office 2007 SP2 or greater providing they have installed the latest Office 2003 service pack, and the latest Microsoft Office Compatibility Pack. A technical document is available at http://technet.microsoft.com/en-us/library/cc179125.aspx

Revision	Name	Date
Version 1	Matthew Sparks, LCSS	1/5/12
Version 1.1 – changes recommended by DISAG	Matthew Sparks, LCSS	31/5/12