RM Framework Guidance Document: Data Protection Breaches

The aim of this guidance is to help staff to:

1. identify when a data breach involving personal data has taken place;
2. understand the main causes for data protection breaches, and how these can be minimised;
3. take appropriate action in the event of a data breach occurring involving personal data.

As a Data Controller the University has specific duties and obligations for how it handles data breaches involving personal data.

This guidance is intended to highlight the role of the **Governance and Information Compliance Team** in responding to such breaches; it is not intended to be a comprehensive guide to information security.

Data Protection Breach?

"A Data Protection Breach occurs when personal data is handled contrary to the principles of the Data Protection Act. In particular where personal information is lost, copied, transmitted, viewed, stolen or used by an individual unauthorized to do so."

Examples include:

1. Emailing personal data to the wrong recipient
2. Losing personal data ie on a memory stick, a laptop, or a notebook
3. Accidentally disclosing personal data to an unauthorised person over the phone
4. Leaving hard copy documents at a printer or in another public / shared space

Top Ten Tips: How to avoid a Data Breach

1. **Don't get complacent** – make sure you can identify when you are handling personal data. Ensure you have watched the staff training podcasts: **Data Protection Podcasts**
2. **Attend a Data Protection Training Course**
3. **Offer data protection training and include guidance on protecting personal data in your staff induction programme**
4. **Ensure all access rights to staff who no longer work in your department are closed.** This includes people who leave the University and staff who move to another department
5. **Use physical security measures.** Make sure cupboards, filing cabinets, secure rooms etc are kept locked, don't leave keys on display
6. **Use strong passwords:** You can find out more about how to keep your password secure on the Information Services web page here: **IS Password Management**
7. **Take special care with emails** – this is the most common cause of breaches (see further email guidance below)
8. **Save sensibly:** Ensure you always save documents to the University Filestore (Drive R/S/Z) and not to the local machine drive (C)
9. **Always confirm the identity of a person before disclosing personal data.** This is necessary in all circumstances, whether by phone, email or face to face.
10. **Dispose of records appropriately**. If you have confidential or sensitive waste then shred it securely

What to do if you have a Data Protection Breach?

Data protection breaches are NEVER planned, but our response to dealing with them is.

We can often minimise the consequences of a data protection breach by taking swift and appropriate action. The Governance and Information Compliance Team will work with any school or department who experiences a data protection breach in fulfilling the following steps as recommended by the Information Commissioner.

Here's what to do if a breach occurs:

1. **Report it! Contact the Governance & Information Compliance Team straightaway at: data-protection@notingham.ac.uk**

   The report should include the nature of the breach i.e. was the data lost, stolen shared or unlawfully processed? What was the content of the data and how many people will be affected? Don't keep it to yourself. Silence may result in more harm. The Governance and Information Compliance Team will guide you through the necessary steps to be taken.

2. **Contain it! What you can do to help contain the data breach**

   If the breach is still occurring some immediate actions may be needed to contain it. This is a time-critical part of the process.
   - decide who should take the lead on carrying out a thorough investigation of the breach
   - attempt to recover lost equipment
   - identify recipients of the breached data and instruct them to delete it
   - change any passwords or entry codes immediately
   - establish who needs to be informed

3. **Carry out a Risk Assessment**. A risk assessment will identify what type of data was involved, whether it could be put to inappropriate use, the number of individuals (or organisations) affected, any harm that could result and any wider consequences as a result of the breach.

Here's what you must do following a data breach:

4. **Review and Evaluate.** This will include:
   a. the causes of the breach
   b. the effectiveness of the response to the breach
   c. any risks of the breach occurring again
   d. how policies can be strengthened to prevent future breaches; and
   e. staff awareness and whether further training is needed

The Governance and Information Compliance Team keep a log of all breaches involving personal data and copies of all incident investigations. They will determine who needs to be notified and any communications that will need to be sent. This may involve contacting individuals and in extreme cases the Information Commissioner.

Top Tips for managing emails to prevent breaches

Around 40% of data breaches occur through human error. The most frequent occurrence is through email. Here's how to avoid unnecessary email mistakes.

1. **Don't email sensitive, confidential or personal data if you don't need to.**
2. **Password Protect.** If you need to send an email that contains personal data, ensure this is placed in a password protected attachment – never in the body of the email. Give the recipient the password over the phone, and never in the same email.
3. **Double-check you have the right recipient.** There are many staff and students at the University who share the same name. If you send an email containing personal data to the wrong recipient it's a data breach. Always check you have the correct email address, don't assume outlook has found the right recipient, if in doubt call them first.
4. **Don't open suspicious emails.** Phishing email messages are designed to steal your identity. They ask for personal data, or direct you to websites or phone numbers to call where they ask you to provide personal data. If you suspect an email is suspicious, don't open it and forward it immediately to: **itservicedesk@nottingham.ac.uk**
5. **Use a Strong Password.** These should be a minimum of eight characters and contain a combination of letters and numbers. You can find out more about managing your password here: **IS Password Management**
6. **Always lock your screen whenever you leave your desk.** You can do this by pressing > CTRL –ALT – DELETE and selecting 'Lock this computer.'

Remember: All emails are records and may be disclosed through our legal obligations under the Data Protection and Freedom of Information Acts.

The University has produced extensive guidance about email usage. Please refer to this guidance at:

http://www.nottingham.ac.uk/hr/guidesandsupport/universitycodesofpracticeandrules/electronicmailusage.aspx

How do I password protect a document?

You can protect a document by using a password to help prevent unauthorized access. The following guidance is for Microsoft Windows 7 device using Microsoft Office 2010.

1. Click the **File** tab.
2. Click **Info**.
3. Click **Protect Document**, and then click **Encrypt with Password**.
4. In the **Encrypt Document** box, type a password, and then click **OK**.
5. In the **Confirm Password** box, type the password again, and then click **OK**.

Passwords are case-sensitive. Make sure that the CAPS LOCK key is turned off when you enter a password for the first time. Remember, if you lose or forget a password, there is no way to recover the password once it has been lost.

Further Information

Information Commissioner:

Guidance on data security breach management

The University of Nottingham:

Data Protection Policy

Records and Information Compliance Webpages

For further information about this guidance document contact:

Jenny Rochfort
Information and Records Manager
Jennifer.rochfort@nottingham.ac.uk
0115 7484017