University of BRISTOL

POSITIVE WORKING environment

Data security at the University of Bristol

Data security is not optional

www.bris.ac.uk/infosec

What has data security got to do with me?

An important part of developing our Positive Working Environment (www.bristol.ac.uk/pwe) at Bristol includes not only our legal responsibilities with respect to data, but also having the highest levels of respect for all information that relates to colleagues, students, research clients and a whole range of other contacts.

What are the most common reasons for data security breaches?

Research into data breaches in HE institutions indicates that the majority of incidents are due to:

- Unauthorised access by staff – both accidental and malicious.
- Accidental exposure of data online.
- Theft or loss of laptop, mobile device, storage media or briefcase.

How do I keep my personal data safe?

Personal Security

Keeping data secure mainly requires common sense. Keep your own personal data as secure as you can – in fact look after it as carefully as you look after your wallet or purse. Remember:

- Never reveal your passwords to anyone.
- Be very careful with information you put on social networking websites, such as Facebook.

Further information is available at www.bristol.ac.uk/infosec/protectyou.

Handling University data: some FAQs

I need to work away from the office – what is or isn't acceptable practice?

- Do not use your personal laptop or computer to store or process restricted data.
- If necessary arrange access to a University fully disk-encrypted laptop.

Visit www.bristol.ac.uk/infosec/uobdata/encrypt for advice about encryption.

- It is acceptable to use your home computer providing that you process the restricted data via a remote desktop terminal server, as the actual processing is done on the University server and not on your computer. Remember not to save or transfer data onto your home computer.

I only use my University PC or laptop at my desk – what do I need to know?

- All computers are vulnerable to attack and you should ensure that you are fully protected and use common sense when using the Internet or downloading or receiving information from unknown sources. See www.bristol.ac.uk/infosec/protectpc for further information.
- The Information Commissioner has ruled that institutions are liable under the Data Protection Act for the loss of data by theft and any laptop, storage device or similar, which is used to hold or process confidential data, should be fully disk-encrypted even if it is kept on your desk.

Can I send restricted data by ordinary email or via fluff?

- Sending this sort of data by email could be considered a breach of confidentiality.
- You should never use a personal email account for conducting University business.
- If there is no alternative to email, ensure that confidential data is effectively encrypted.
- All movement of restricted data, outside of the University network, must only be done via encrypted files or within encrypted drives.

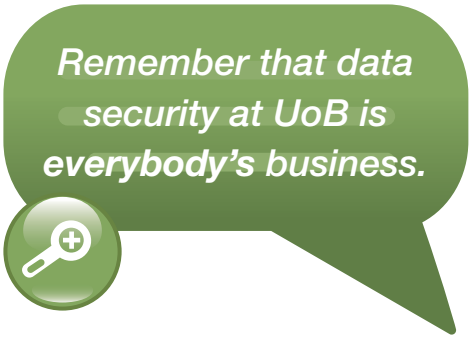
What are the consequences of data loss?

Under the Data Protection Act, the University could be fined with the amount based on the severity of the loss and the type of data involved. The impact on the reputation of the University and harm to individuals could be far worse. From 6th April 2010 the maximum penalty which can be imposed on an organisation by the Information Commissioner's Office is £500,000.

Does this mean that I have to keep all University data secure?

Different types of data require different levels of security, these levels being dependent on the risk of harm to the University or individuals if this data were to be leaked or lost.

There are five categories of data – Public, Open, Confidential, Strictly confidential and Secret.



Data that is deemed to be Public, or small quantities of Open data would generally not constitute a threat if lost or leaked. In general, data about identifiable individuals or data, which, if leaked, could cause harm to the University or individuals should be considered Confidential or Secret. To see examples of the different types of data visit www.bristol.ac.uk/infosec/uobdata/classifications.

If you're not sure whether the data that you use is rated as Confidential or above, seek advice from the Information Rights Officer, www.bristol.ac.uk/secretary/dataprotection.

Think about the following questions before moving restricted data:

- Why am I sending/carrying this data?
- Do I need to send/carry all of this data or only a part of it?
- Does the person I am sending this to really need this data?
- Are there ways that I can make this process more secure?

It can take **seconds** *to give away your identity, but it can take* **years** *to fully recover.*

University of BRISTOL

TOP 10 DATA SECURITY TIPS

- ☑ Know what constitutes restricted UoB data
- ☑ Process restricted data on secure UoB computers only and do not store restricted data on non-UoB equipment
- ☑ Encrypt restricted data to transport it and fully disk encrypt your laptop/netbook
- ☑ Share restricted data only with those with the right and need to view it
- ☑ Do not make copies of restricted data
- ☑ Lock away unsecured restricted data and lock your door if leaving your room unattended
- ☑ Never share or disclose your UoB password or use it for non-UoB services
- ☑ For UoB business use your UoB email account and a UoB recommended secure email client
- ☑ Securely erase data before disposing of hardware and storage
- ☑ If in doubt about data, ask advice from the Information Rights Officer based in the University Secretary's Office