Appendix A - Information Handling Guidance

Appendix A - Information Handling Guidance

1. Scope and Purpose

The purpose of this Information Handling Guidance, and the associated Information Security Policy, is not to constrain ways of working, but to enable University employees to fulfill their duties securely without putting themselves or the University at risk of disclosing sensitive data. Individuals are responsible and liable for the information they handle, therefore all University employees should read, understand and adhere to this Guidance.

2. Classifying Information

The University has established a simple classification dividing information into either sensitive or non-sensitive. Information may be classed as sensitive if it contains:

- Personal information including sexuality, disability, race, political affiliation, age, salary, criminal convictions. Other personal information could include home address or photographs. If an individual can identify themselves uniquely from any set of data this too must be treated as sensitive data. *(Data Protection Act definition)*
- Any information likely to harm the University commercially if it got into the public domain. This may include 'trade' secrets, financial information, intellectual property and research data. *(Freedom Of Information definition)*
- Internal and confidential information not yet in the public domain.

If in doubt, treat as sensitive.

3. General Principles (Information Security Policy)

- The University will only store, process, retain and disclose information in accordance with the requirements of the Data Protection Act.
- Employees should ensure information is stored, read, heard, edited, accessed and otherwise used by only those who have the right to do so.
- Areas and offices where sensitive information is processed shall be given an appropriate level of physical security and access control.
- The University encourages a clear desk and screen policy.
- The removal or transfer of all sensitive information should be authorised by the appropriate line manager.
- Sensitive information held on laptops, tablets, USB devices or other storage media must be encrypted using University prescribed software.
- Sensitive information may only be transferred when the confidentiality and integrity of the data can be assured, and digital information must be encrypted.
- If you believe that sensitive information has been lost, or identify a potential information security risk, immediately inform your line manager, Dean or Director.
- Seek further advice a from your line manager if you are unsure about any aspect of handling sensitive information and feedback to help improve this Guidance.

4. Physical Security

- Your University provided workstation (PC, Mac, laptop, tablet or other device) should be secured and your office locked at night.
- If you take your University laptop or tablet off-campus, home or away on business, keep it secure at all times.
- Other University devices such as PDAs and mobile phones, and storage media including USB drives and CDs should be kept secure at all times.

5. Laptops & Tablets

- It is not permitted to store sensitive University information on a personal / user-owned laptop or tablet device.
- If your University provided laptop or tablet is used to store sensitive information required for your work it must be encrypted using University prescribed software.

6. Mobile Phones, Smart Phones and PDAs

- It is not permitted to store sensitive University information on mobile phones, smart phones or PDAs.
- Personal / user-owned mobile phones, smart phones or PDA devices may be used to view University email and (if required) sensitive information, but should be protected with a password or pin code and must not be used to store content.
- University provided mobile devices, that do not support encryption, must be protected a password or pin code.

7. USB Devices (inc external hard drives, pen drives and memory sticks)

- If your USB device is used to store sensitive information required for your work it must be encrypted using University approved software.

8. CDs, DVDs and other media

- Where there is a requirement to transfer sensitive information on a CD, DVD or other media you must encrypt the data file or document using University approved software.
- Consider using registered post or approved couriers if the encrypted media is to be distributed to another individual or organisation, and ensure the recipient is known to you, and that they are entitled to receive it.

9. Email and Attachments

- Given the potential risks associated with email communications, sensitive information should not be sent outside of the University via email unless there is a strong business need.
- Where there is a justifiable requirement use University prescribed software to encrypt the information as an attachment (do not communicate sensitive information in the main body of the email).
- The use of long and complex encryption passwords or phrases is recommended. These should be communicated to the (known) recipient as a separate correspondence – ideally via telephone or text.
- Double check the recipients email address before hitting the send button.