University of Hertfordshire

**MANAGING PERSONAL AND CONFIDENTIAL INFORMATION (PCi)** **v2 (December 2011)**

This Staff Guidance applies to the management and processing (ie creation, use, disclosure, dissemination and storage) of person identifiable information and other confidential and commercially sensitive information, data and documents both printed and electronic**.**

This guidance sets out how you can process Personal & Confidential Information (PCi) safely. It supports the policies and principles set out in the University Information Management Policy (UPR IM02), Information Security Policy (UPR IM03), Data Management Policy (UPR IM12) and the Records Management Standards.

You must:

- have a legitimate professional reason related to your job to be handling PCi
- comply with University requirements for managing and processing PCi
- be able to justify using PCi on a laptop or portable media device or in a public space
- seek advice from the Chief Information Officer about any PCi use not covered by this guidance

| **Acceptable Practice** | | **Unacceptable Practice** |
|---|---|---|
| **1 Saving and storage of PCi** | | |
| • All PCi must be saved and stored in the agreed official University files; primarily the corporate MIS software systems; the staff network S: drives; paper files in Registry, OVC, Finance and HR<br>• PCi should only be stored short term on the C:drive of a University computer |   | • Saving PCi on a non-University computer<br>• Encrypting the master copy of any data |
| **2 Laptop security** | | |
| • Laptops must be configured to require individual login and default to power save mode with re-login within 10 min of non-use<br>• Laptops must be shut down or workstation lock mode applied when not in use (Ctrl Alt Delete)<br>• Laptops must be kept secure and safe at all times and locked away when not in use |  | • Using a laptop in a public space without assessing the risk of compromise to PCi<br>• Allowing anyone else to use your University laptop or your login |
| **3 Use of portable media devices (eg datasticks, external hard drives, CD/DVDs, cameras, phones)** | | |
| • PCi may only be stored on encrypted data sticks for transfer purposes and then deleted immediately the transfer has taken place<br>• Images on cameras or phones must be transferred to official University files as soon as possible and then deleted from the portable device |   | • Use of portable media devices to store or backup PCi<br>• Regular transfer or unencrypted transfer of PCi via portable media |
| **4 Sending portable media (eg CD/DVDs, Data Sticks) or printed documents by post or courier** | | |
| • PCi should only be sent by post or courier as a transfer method of last resort<br>• Only the minimum PCi required should be sent<br>• PCi in electronic format on portable media must be encrypted<br>• Secure packaging and recorded or courier delivery must be used<br>• Dated and timed sign-out and sign-received confirmations must be kept for tracking purposes |   | • Sending unencrypted PCi<br>• Sending in standard envelope by regular post |

| Acceptable Practice | | Unacceptable Practice |
|---|---|---|
| **5 Sending PCi by email or via 'cloud' services** | | |
| • Sending PCi by email or via 'cloud' services such as Dropbox should be avoided if possible<br>• PCi may only be sent by email in an encrypted attachment and to an agreed named recipient with a recognised valid email address<br>• Exceptionally, PCi may be sent in an unencrypted email attachment between individual named UH staff using UH email addresses within the MS Exchange staff email service |  | • Sending PCi in the body of an email<br>• Sending PCi by email to general or unrecognised email addresses<br>• Transfering PCi via third parties |
| **6 Access to electronic PCi from off-campus and over UH wireless networks** | | |
| • All access to and use of PCi from off-campus and over UH wireless networks must be via the University VPN service (https://uhvpn.herts.ac.uk)<br>• PCi downloaded via the VPN service for local use must not be retained locally. PCi files must be re-uploaded to University corporate systems and storage via the VPN service immediately after use |  | • Non-secure access to PCi from off-campus |
| **7 Access by externals to University online systems and services containing PCi** | | |
| • Access is only available to individuals who have been granted University Membership B status and a personal University login account with approved access to specific PCi |  | • Borrowing a login account from a member of University staff |
| **8 Use of PCi by recipients external to the University** | | |
| • All use of PCi by external recipients must be in accordance with University Data Protection and Privacy Policies<br>• External recipients must have a legitimate professional reason for processing PCi<br>• Transfering PCi to an external recipient must be authorised in advance using a University Data Access / Sharing Agreement and signed off by the appropriate Data Steward<br>• The duty of confidentiality must be understood and applied by the external recipient |  | • Unauthorised transfer of PCi to an external receipt<br>• Unauthorised receipt or use of PCi by an external recipient<br>• Disclosure of PCi by the external recipient<br>• Retention of PCi beyond the agreed period |
| **9 Disposal of computers, software, data files and documents** | | |
| • All desktop and laptop computers, software, datafiles and documents must be disposed of in line with University policy agreed retention periods and procedures |  | • Computers or documents left lying around in offices and storerooms |
| **10 Sending of hard drives to third parties for maintenance, file recovery, etc** | | |
| • Advice must be sought from the Chief Information Officer<br>• Risk assessment must be carried out |  | • Use of unofficial third parties |

Please also refer to:
- the University instructions for downloading and using TrueCrypt encryption
- the University Data Access / Sharing Agreement form (*available on the StudyNet Information Management staff intranet site*)