**Information Handling Protocol**

General principles:

1) Wherever possible always aim to keep **'restricted'** and **'highly restricted'** information within the University's secure environment/systems.
2) Where this is not possible consider whether the restricted information can be **redacted** or **anonymised**. If this is not possible, appropriate security measures should be implemented (for example agents on mobile devices containing personal data and appropriate physical security measures for paper records). For the most confidential data (and where a funder requires) discuss with Computing Services about encryption.
3) Any potential loss or unauthorised disclosure of **personal data** and or **sensitive personal data** must be reported to the University's Data Protection Officer (the Senior Legal Adviser).

| **Location/format of information** | **Highly restricted** | **Restricted** | **Internal use** |
|---|---|---|---|
| Shared file storage areas on University's network (e.g. shared windows folders) | Strictly restricted access on a need to know basis. | Limit number of, and identify, individuals who have access to folders. | No internal restrictions |
| Department/local based server | No storage or creation permitted unless server environment is equivalent to Computing Services (BUCS) server security environment. Advice must be sought from local IT support concerning access rights, physical security and back-up. | No storage or creation permitted unless server environment is equivalent to Computing Services (BUCS) server security environment. Advice must be sought from local IT support concerning access rights, physical security and back-up. | If local server is required, advice must be sought from local IT support concerning access rights, physical security and back-up. |
| University desktop PCs hard drive (C drive) | Avoid storing data here (use remote drives). | Avoid storing data here (use remote drives). | Manual back up required. |
| Specialist MI systems (e.g. SAMIS, I Trent, Pure etc) | Administrators to ensure access rights appropriately controlled. All managers to ensure access removed when staff member leaves.<br>Appropriate security measures must be taken if data extracted from system. | Administrators to ensure access rights appropriately controlled. All managers to ensure access removed when staff member leaves.<br>Appropriate security measures must be taken if data extracted from system. | No restrictions (MIS information will principally fall in the other categories) |

| Location/format of information | Highly restricted | Restricted | Internal use |
|---|---|---|---|
| University owned laptop or mobile devices (e.g. IPad or smart phone, portable storage devices) | Devices must have wiping agents installed. For the most sensitive data encryption should be considered (contact Computing Services for advice).<br>Use secure remote connection.<br>Never use public wifi. If in doubt about use of public wifi, consult Computing Services.<br>Do not leave logged on and unattended.<br>Do not work on files in public areas.<br>Do not share use of laptop/device with non-University staff.<br>Anti-malware software should be kept up to date | Devices should have wiping agents installed where possible<br>Use secure remote connection.<br>Avoid use of public wifi as far as possible.<br>Do not leave logged on and unattended.<br>Take great care if working on files in public areas.<br>Do not share use of laptop/device with non-University staff.<br>Anti-malware software should be kept up to date | Use secure remote connection wherever possible.<br>Do not leave logged on and unattended.<br>Do not share use of laptop/device with non-University staff.<br>Anti-malware software should be kept up to date |
| Personally owned desktop PC, laptop or mobile device (e.g. IPad or smart phone, portable storage devices) | May be used via secure remote connection if used in a private environment. Mobile devices must have wiping agent installed. Never use public wifi. If in doubt about use of public wifi, consult Computing Services. Do not save files to local storage area/non-University owned unencrypted device.<br>Do not leave logged in and unattended. | May be used via secure remote connection if used in a private environment. Avoid use of public wifi as far as possible.<br>If you need to save files to local storage area/non-University owned device ensure they are deleted at the earliest opportunity. Consider secure erasing most sensitive files (please contact Computing Services for more advice about this).<br>Do not leave logged in and unattended. | May be used via secure remote connection if used in a private environment.<br><br>Do not leave logged in and unattended. |
| External 'cloud' storage outside of University agreed contract e.g. individually set up drop box accounts | Avoid using– consider University solutions/seek advice from Computing Services | Avoid using where possible - consider University solutions/seek advice from Computing Services. | Use University solutions wherever possible. |
| Sending email from | Check recipient(s) are correct. | Check recipient(s) are correct. | No restrictions |

| | | | |
|---|---|---|---|
| University hosted account to another | | | |
| Sending email from University hosted account to an external account | Double check recipient(s) are correct.<br>Auto-forwarding to external account should be avoided.<br>Consider secure alternatives to using e-mail (seek advice from Computing Services)<br>For the most sensitive information, consider password encryption of file with strong password (8+ character, mixed character), | Check recipient(s) are correct.<br><br>Auto-forwarding to external account should be avoided. | Check recipient(s) are correct. |
| Sending email from externally provided personal account (e.g. gmail) | Avoid (please be aware that any data in sent items or your inbox will be stored outside of University's secure systems). | Avoid (please be aware that any data in sent items or your inbox will be stored outside of University's secure systems). | Use University or other organisations' email accounts wherever possible (please be aware that any data in sent items or your inbox will be stored outside of University's secure systems). |
| Paper copies | Must be stored in secure environment e.g. locked cabinet/drawer. Must not be left unattended in an insecure environment.<br>Must be disposed of securely (e.g. confidential shredder). | Should be stored in secure environment e.g. locked cabinet/drawer.<br>Should not be left unattended in an insecure environment.<br>Should be disposed of securely (e.g. confidential shredder). | No restrictions |
| Internal post service | Avoid where possible (e.g. deliver in person by hand).If internal post must be used please ensure that a sealed envelope is used and marked 'highly restricted' with sender details. | Sealed envelope marked 'restricted' with sender details. | No restrictions |
| External post service | Tracked and delivery recorded service, marked 'highly restricted'. | Consider tracked and delivery recorded service where appropriate and marked 'restricted'. | No restrictions |
| Fax machine | Only use if recipient has verified security of receiving machine and is at machine awaiting receipt. Double check number. Use cover sheet. | Only use if recipient has verified security of receiving machine. | No restrictions |