Our staff will often have stewardship of personal information about other people. The University has some obligations with respect to keeping this information safe and secure. As our employee or contractor you are accountable for the Personal Information that you have stewardship of at various times.

This document is intended to provide you with guidance regarding how you should protect this information when you store it on computer equipment, portable USB sticks or other devices. For day to day purposes it is best to assume that all information about a living, identifiable individual is personal information and it is to this that the document refers.

**Staff Responsibilities: Individuals must be able to justify the use of any Personal Information and the use must be relevant to your job**

If any of the guidance below restricts or prevents you using Personal Information to do your job effectively and you believe there is a justifiable reason to process the data you should contact the Head of Information Governance for advice.

<table>
<thead>
<tr>
<th>Good Practice</th>
<th>Dangerous Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1) Saving and storage of Personal Information</strong></td>
<td><strong>2) USB Sticks, Cameras and other digital capture devices, Personal Digital Assistants (PDAs), Mobile Phones</strong></td>
</tr>
<tr>
<td>- Personal Information should be stored on shared drives or the Business Application hosted on the University network.</td>
<td>- Saving Personal Information on the C: drive of a laptop and or mobile device unencrypted</td>
</tr>
<tr>
<td>- If Personal Information is saved on the local drive of a portable computer it should be encrypted. The Service Desk can advise on how to encrypt local data.</td>
<td>- Not ensuring that personal information stored on paper is properly secured</td>
</tr>
<tr>
<td>- The University will no longer sell devices that do not support encryption of data and University staff should no longer support such devices.</td>
<td>- Not backing up encrypted Personal Information on a regular basis</td>
</tr>
<tr>
<td>- Personal Information should be backed up on a regular basis to the University network by the user</td>
<td>- Using or supporting the use of an unencrypted device</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>3) Laptop Computer Security</strong></th>
<th><strong>3) Laptop Computer Security</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Accountability for University-supplied Laptop Computers and the data on them falls to the person to whom the device was issued. Any change in ownership should be notified to the IS Service Desk who will update the University asset register with the change of accountability.</td>
<td>- Using a laptop or mobile device in a public place without assessing the situation to ensure that others might not see information to which they may not be privy</td>
</tr>
<tr>
<td>- Accountability for data on privately owned Laptop Computers lies with the staff member or company who owns the Laptop. Any change of ownership will not change the accountability for the safety of Personal Information that is under your stewardship as an employee or contractor to City University.</td>
<td>- Passing your University-Supplied Laptop computer to someone else’s care without notifying the IS Service Desk.</td>
</tr>
<tr>
<td>- Personal Information stored on USB sticks should be encrypted and deleted once the transfer has taken place</td>
<td>- Passing your privately owned computer to somebody else’s care while it contains Personal Information.</td>
</tr>
<tr>
<td>- Images captured for University purposes should be transferred to a University server as soon as possible</td>
<td>- On PDAs and Mobile Phones you should use a PIN to prevent unauthorised access.</td>
</tr>
</tbody>
</table>

Authorised by: Chief Information officer
Good Practice

- Be aware of the safe storage of Laptop computers when not being used. It is advisable that you use a desk lock to secure the device when you are not in the office.
- You should use a password screensaver on your laptop to prevent unauthorised access when the device is idle for any significant period of time.
- You should ensure that your laptop cannot be booted without a password.

5) Sending portable media by post (CD/DVD/USB Stick)
- Only the minimum Personal Information should be sent
- All Personal Information data should be encrypted. If not possible use secure packaging and recorded delivery (subject to risk assessment)

6) Personal Information in email
- You should consider carefully the information that you share using email and the ultimate possible destination of that information.

7) Recipients external to the University – use of Personal Information
- The recipient must have a legitimate need for the data
- Sharing agreements should be in place where there is a regular flow of Personal Information
- You should ensure that there is a duty of confidentiality that is fully understood by the recipient
- The recipient should be aware that they are not authorised to disclose the information without permission

8) Remote Access
- Access of Personal Information using technologies supplied by the Information Services Department.
- Take care when entering usernames and passwords that others do not see them.
- Ensure that access to personal information is not done where unauthorised people might be able to view that information.

9) PC Disposal/System Maintenance
- All PC and laptops should be disposed in line with University policy. For disposal contact the IS Service Desk. Information Services will ensure that Personal Information cannot be accessed on these devices and that they are rendered safe for use or disposal outside the University.

10) Equipment Loss
- Any equipment loss must be reported immediately to the IS Service Desk
- If you have “remote wipe” installed on the device, activate this as soon as possible after the loss.

Dangerous Practice

- Not cleaning any City University related Personal Information from your laptop computer after your contractual relationship with City University is finished.
- Not securing your laptop computer adequately when you are not using it.
- Not securing the data on your Laptop Computer adequately through use of a password to prevent access.

- Sending Personal Information unencrypted
- Sending Personal Information in a standard envelope by regular post

- Submitting Personal Information via email using an address that you have not verified as being the responsibility of someone who is appropriate to receive that email.

- Storing/processing Personal Information where there is no legitimate need to share the information with the recipient
- Recipient using Personal Information in a manner not approved by the University
- Any breach of good practice in this area

- Set up or use of remote access services not provided by Information Services

- PCs and Laptops given or sold to anyone without the intervention of Information Services
- PCs and Laptops left unused for extended periods in offices, store rooms etc.

- Not reporting the loss of computer equipment or data as soon as possible after the event.