All usersmust protect personal data and information assets by following the procedures below:

1. **Locking screens** when away from their desks (using Windows Button + L)
2. By maintaining a **clear desk** whenever possible, by using drawers or cupboards (lockable wherever possible) when leaving the desk unattended.
3. **Disposing of information and equipment** in an appropriate manner:
   1. Equipment – via the organisation’s accredited provider
   2. Paper – using either a crosscut shredder or the confidential waste bins.
4. Ensuring **special categories of personal data** are given extra security, and at a minimum data is locked away when not in use.
5. Using encryption when **working with personal data offsite** e.g. working at home (on an encrypted device or an encrypted USB stick owned by the organisation). For encrypted USB sticks, users must:
   1. Ensure the information is uploaded back to the organisation’s network as soon as possible; and
   2. Not process or save the data locally to any devices not owned by the organisation.
6. Ensuring when processing data on a **personal / non-organisation device** that:
   1. The device is protected by PIN, password or fingerprint, and ideally encrypted
   2. The organisation’s systems (e.g. Webmail) are not left logged in
   3. A separate email app is used to access work emails (i.e. not merged with personal emails)
   4. Attachments are not opened (and downloaded), unless in an emergency, when measures must be taken to delete the information after use
7. Always protecting hardcopy personal data when **taken offsite**. Users must:
   1. Keep information and equipment on their person at all times (e.g. when stopping off on the way home)
   2. Transport data in an appropriate receptacle (e.g. bag) to reduce the risk of opportunistic theft
   3. Not leave the information and equipment on display in a vehicle when not in use
   4. Consider where data could be minimised. For example for trips:
      1. Not making the information personally identifiable, by using pseudonymisation (e.g. Unique reference or initials)
      2. Using a code system or colour code system to identify key indicators (e.g. allergies)
      3. Not having the organisation logo on any hardcopy documents
   5. Consider encryption to protect the data (e.g. encrypted device rather than hard copies)
8. Ensuring care is taken with **emails**, by applying the following:
   1. Was I expecting this email? Does it look and feel right?
   2. Can I check (by other trusted means) that the email is legitimate?
   3. Don’t click any links or open any attachments with validating them
   4. Use blind copy (BCC) when emailing more than one external user
   5. Double check the email address for accuracy before sending
   6. Encrypt personal data to external addresses ([See Appendix 1](#SecureEmail))
   7. Use an email delay rule on all emails sent
9. Taking care when connected an **electronic whiteboard or projector**.
   1. Do not access emails or any system containing personal data (e.g. MIS, safeguarding, etc) whilst connected
   2. Be vigilant when entering logins and passwords, and avoid doing this whilst connected
   3. Freeze the screen if appropriate
10. Ensuring any **information disclosed verbally** is
    1. Validated – the person calling/present is known to have the need to know
    2. Documented – a summary of what was disclosed should be kept and filed
11. Ensuring any information sent **via post** is secure
    1. Double check the address - where possible copy and paste from a verified source
    2. Mark as Private & Confidential
    3. Use recorded delivery

**Appendix** **1 – Securing an email in transit**

The three main risks associated with email are:

1. Emails are intercepted in transit
2. Emails are sent to the wrong recipient
3. Email addresses are disclosed to those without the need to know

This process covers risk (1) and enables the secure exchange of information over email (in the absence of a secure email portal).

1. Document the information in an MS Office document
2. Ensure that this is not the source/primary document – if it is then create a copy

*Do not encrypt the source document – if you do and then forget the password you are unlikely to be able to gain access to the information again!*

1. Have the document open, and then click
   1. File
   2. Protect Document
   3. Encrypt with Password
   4. Create a strong password (minimum of 8 characters) – you could use a password generator <https://passwordsgenerator.net/> or pre-agree one with the recipient
   5. Apply this password to the document
   6. Save
2. Attach the secured document to an email and send it to the recipient
3. Communicate the password by other trusted means e.g. Phone call or text message. Before disclosing the password ensure you:
   1. Are communicating with the correct person; and
   2. Confirm that they have received the email

*It should be noted that encrypted attachments are sometimes blocked by email gateways as they cannot inspect the contents*