IINFORMATION GOVERNANCE TOOLKIT POLICIES: DATA PROTECTION INFORMATION

Laptop

- Confidential information should not be taken off site.
- Laptops should be locked away in the building when not in use.
- Where it is necessary to take confidential information off site, remember:
  - Do not leave the laptop unattended
  - Remove confidential information as soon as possible
  - Password protect files containing confidential information
  - Ensure regular housekeeping of laptop files

Computer

- Be careful where you site your computer screen: ensure any confidential or personal information cannot be accidentally or deliberately seen by visitors or staff who do not have authorised access.
- Always keep your password confidential and do not write it down.
- Do not share passwords; this may be a disciplinary offence.
- Change your password regularly; most systems will force a regular change of password and designate the format of it.
- Remember to log off your computer when leaving the office, or use password protected screen savers for short absences.
- Any user who suspects they may have a computer virus must report it immediately to their IT helpdesk/Practice/System Manager.
- Any disk or CD coming into the organisation – no matter where it has come from – must be virus checked before use.

Database

- Ensure that any database that is created is in line with the organisation's Data Protection Notification details.
- Inform the Data Protection Officer when new databases are created or introduced to your department/service.

Telephone

- Be careful about leaving messages on answerphones.
- Be careful when taking messages off answerphones And ensure that messages cannot be overheard whilst being played back.
- When receiving calls requesting personal information:
  - Verify the identity of the caller
  - Ask for a reason for the request
  - If in doubt as to whether information should be disclosed tell the caller you will call them back. Take advice from your manager.
  - Call back to main switchboard or known and trusted numbers only – not direct lines you do not recognise or mobile telephones

Faxing

- Do not fax personal or confidential information unless it is absolutely necessary.
- If it is necessary, ensure that you fax the information to a Safe Haven/Secure fax.
- If faxing personal or confidential information:
  - Double check the fax number
  - Ask the recipient to confirm receipt of the fax
  - Ensure you mark the fax header "Private and Confidential"

South
collective thinking

IINFORMATION GOVERNANCE TOOLKIT POLICIES: DATA PROTECTION INFORMATION

Email

- Patient identifiable information should not be sent via e-mail unless the message is encrypted.

Post

- Ensure envelopes are marked “Private and Confidential”.
- Double check the full postal address of the recipient.
- Choose a secure method for sending confidential information through the external post e.g. recorded delivery.
- When necessary ask the recipient to confirm receipt.
- Ensure that incoming confidential post is handled appropriately.

Printer

- Avoid printing confidential/personal information to central printers.
- Keep the number of copies to a minimum.

Photocopying

- Do not make excessive copies of confidential information.
- Regularly check /update your distribution list to ensure copies are not sent to staff who have left or moved to another service.

Bin

- Be sure that you dispose of confidential information appropriately.
- All personal information is confidential and must be shredded.
- Confidential waste paper must not be used as scrap paper for messages, notes etc.

Filing Cabinet

- Ensure that filing cabinets containing confidential information are always kept locked when not in immediate use.
- Ensure filing cabinets are not sited in areas which are accessible to members of the public/visitors.
- Ensure regular housekeeping of your files.
- When destroying information ensure you comply with NHS retention guidelines.

Office

- Remember to lock and secure the office when it is unattended and at the end of the day.
- Whenever possible escort visitors at all times on site.
- Remember to wear your identity badge.

Desk

- Operate a clear desk policy, especially when hot desking or working in an open plan office.
- Do not leave confidential information unattended or out overnight – particularly important when hot desking or working in an open plan office.

Person

- Ensure you hold confidential conversations in an appropriate place. Inappropriate places include corridors, open plan offices, and at the photocopier!
- Gain the patient’s consent before sharing their personal information with relatives.