Rules for handling personal data
All staff

Computer security

- Don’t share your passwords
- Don’t set up passwords which are then automatically remembered by the device
- Lock your laptop/tablet/device whenever you leave it

Personal data

- Only ***store*** sensitive data on encrypted College-owned fixed or portable devices
- Be aware when sharing personal data – ask what, why and how (don’t use third party systems such as DropBox, Mediafire, Wetransfer, etc)
- Use RNCM systems to access your emails and documents
- If a non-College computer is used to ***create or access*** (not store) sensitive information, ensure the computer has up-to-date security protection
- Lock away sensitive papers when you are away from your desk

Data disposal

- Do not keep personal data longer than you need it - follow the RNCM retention schedule
- Dispose of personal data with care - record how and when (use College shredding services/boxes for disposal of paper documents)
- If using your own device, remove any temporary or trash files containing personal data
- Ask IT to dispose of unwanted, damaged or obsolete RNCM computer hardware

What if there’s a problem?

- Incidents happen! Tell us when things are lost, stolen or shared by mistake
- Let the IT department know immediately if you think someone has accessed your password or device

What should I do now?

- Review your electronic and paper files and dispose of anything you shouldn’t keep at all, you’ve kept for too long (see retention schedule) or which is kept by someone else
- Review your emails and attachments and remove anything too old, that you shouldn’t retain or which is retained by someone else
- Access the on-line training course on moodle/intranet