

Rules for handling personal data

Heads and line managers

Personal data

- Only **store** sensitive data on encrypted College-owned fixed or portable devices
- If a non-College computer is used to **create or access** (not store) sensitive information, ensure the computer has up-to-date security protection
- 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
- Lock away sensitive papers when you are away from your desk

What should be kept and by whom?

Type	Detail	Owner
Staff personal files	CV, application, references, formal notes on performance or other issues, sick leave records, PDRs, formal records of numbers of hours/students	HR
Staff personal files	References on employees provided by you Holiday records (pending new HR system) Emergency contact details Job descriptions and personal specifications	You and HR
Student personal files	Progression notes, module/recital marks, absence requests, PLPs, notes on personal issues, personal contact details	Registry
Student personal files	Class allocations/lists, records of prizes, competitions or other awards	You
Alumni files	Records of prizes, competitions, roles/positions, current contact details	You and Development Dept

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 and/or trash files containing personal data
- Ask IT to dispose of unwanted, damaged or obsolete RNCM computer hardware