Data Storage

Identify:

- Importance of data
- Type of data
- Volume of data (Storage space)
- Frequency of changes
- Need of tracking changes
- Importance of fast access
- Do you need remote access
- Collaboration (who needs access)
- Frequency of backup
- Data protection and security policies
- Budget to handle costs

PC/laptop

- Regularly maintain a backup copy of all the data
- Keep working data separate from Raw and Old data
- Develop separate backup solutions for long term storage and frequent / active storage
- Develop shared working solutions for collaborative tasks (e.g. github for code, overleaf for manuscripts) instead of moving/sharing files
- Password protection

Institutional Services/Cloud

Make sure you know the policies related to:

- Backup (Is it backed up, how frequently?)
- Handling of sensitive data (are you allowed to put sensitive data?, encryption policies)
- Versioning (Is the data version controlled?)
- Capacity (What is the maximum allowed storage capacity?)
- Rights and permissions (Sharing with external collaborators)
- Always keep a copy of data elsewhere

Generic Cloud

- May not be secure (not legally allowed)
- May ask for right to use ‘your’ content
- Costly
- Preferably opt for a National/European solution

External portable storage

- Use as a temporary storage
- Regularly test and replace if needed
- Use primarily for data transfer
- Keep another copy on a stable storage medium

Backup of Data

Identify:

- Backup strategy of institute
- Security and Data Protection policies
- The data to backup
- The backup store(s) (3-2-1 rule)
- Frequency of backup maintenance
- Tools for automated backup (if any)
- When to move to archive

Archiving Data

Identify:

- Type of data
    - Use common and sustainable file formats
- Duration to archive the data
- Volume of data
- Documentation of data
- Data integrity checks
- Access (Is the data only stored or an active access is also needed)
- Data protection and security policies
- Trustworthiness and durability of provider