

# Data Storage and Security

Data Management and Sharing Workshop  
Vienna, 14-15 April 2010 WISDOM

# Session topics

- Backing up data
- Storing data
- Keeping data secure

# Backing up data

- Why do back-ups? loss (and change)
- To protect against: software failure, hardware failure, malicious attack, natural disasters
- Different types of back-up
  - Personal data files (e.g., external hard drive)
  - System files (image complete system)

# Considerations in back-ups

- Frequency
- Automatic or manual
- Full, differential, incremental
- Media: CD, DVD, external hard drive, tape, etc.
- Location of back-up media

# Data Storage

- ALL digital storage media are unreliable
- File formats and physical storage media ultimately become obsolete
  - optical (CD, DVD) and magnetic media (hard drive, tapes) degrade

## Best practice:

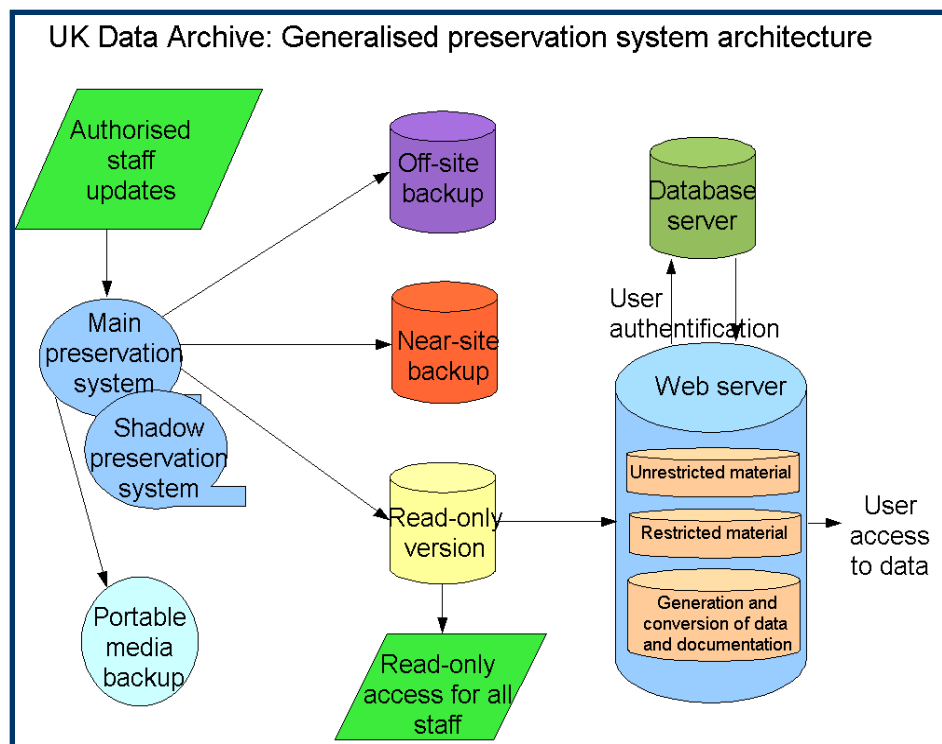
- Use data formats with long-term readability
- Storage strategy with at least two different forms of storage and locations
- Maintain original copy, external local copy and external remote copy
- Copy data files to new media between two and five years after first created
- Check data integrity of stored data files at regular intervals (checksum)
- Know your back-up strategy: institutional/personal; network server/PC/laptop
- Test file recovery
- Know all retention policies that apply: funder, publisher, home institution
- What to protect? Not only data, and not only digital

***And don't forget: data archives are expert in long-term storage***

# Data storage and preservation at UKDA

Multi-copy, multi-storage media and multi version resilience:

- preservation copy (UKDA)
- shadow copy (UKDA)
- dissemination copy to reduce load on main system
- near-site online copy (on campus)
- off-site online copy
- tape-based offline copy (UKDA)



# Data Security

- Protect data from unauthorised access, use, change, disclosure and destruction
- Personal data need more protection, but one system may be easier
- Control physical access to buildings, rooms, cabinets
- Control access to computers
  - Passwords
  - Anti-virus and firewall protection
  - Power surge protection
  - All devices: desktops, laptops, memory sticks, mobile devices
  - All locations: work, home, travel
  - Store most sensitive materials separately (e.g., consent forms)
- Proper disposal of equipment (and rarely, data)
  - Even reformatting the hard drive is **not** sufficient
- But beware of “requirements” to destroy data

# Encryption

- When to use
  - For moving files (e.g., transcriber services)
  - For storing files, especially on mobile devices
- Basic principles
  - Uses an algorithm to transform information (A=1)
  - Need a “key” to decrypt
- Must be easy to use, or won't be used (\*.zip)
- Pretty Good Privacy (PGP) <http://www.pgpi.org/>
- TrueCrypt: <http://www.truecrypt.org/>