Secure Data Disposal Checklist

PA step-by-step guide to protecting your business from data breaches

1. Assess what needs to be disposed

- Identify all devices due for disposal (PCs, laptops, printers, servers, USB sticks, phones, tablets)
- Check for old hard drives or backup tapes stored in cupboards or drawers.
- Review printed records and files that may contain sensitive data.

2. Understand the Risks

- Remember: deleting files is NOT enough - they can often be recovered.
- Know that improper disposal could breach GDPR and result in fines.
- Recognise reputational risk if customer or patient data is exposed.

3. Secure data wiping (Digital Media)

- Use professional software to overwrite drives (minimum 3-pass wipe).
- Encrypt drives before disposal for added protection.
- Obtain certification of data erasure from IT or disposal provider.

4. Physical Destruction when needed

- Shred hard drives, CDs, DVDs, or memory cards using certified equipment.
- Ensure disposal partner is accredited (ISO 27001 / ADISA / equivalent).
- Request a certificate of destruction for your compliance records.

5. Paper Records

- Shred or pulp documents using cross-cut shredders.
- Store shredding in locked consoles until collection.
- Use a secure, GDPR-compliant shredding provider.

6. Vendor / Partner Management

- Verify your disposal provider's credentials and policies.
- Ensure they track custody from collection to destruction.
- Keep certificates and reports for your compliance audit trail.

7**. Staff Awareness**

- Train staff on what counts as sensitive data.
- Include disposal policy in your data protection training.
- Schedule regular refreshers to prevent mistakes.

8. Compliance & Documentation

- Keep records of all disposals (digital and paper).
- Update your data retention policy to reflect disposal actions.
- Store certificates in case of GDPR audits.

✅ **Tip: Build a routine schedule (e.g., quarterly) for checking and securely disposing of old data, rather than waiting for ad-hoc clear-outs.**