

Information Security Checklist

Keeping your computer systems secure can seem like a daunting task but just a few simple changes can really help keep you more secure and protect the data that your business stores and processes.

Physical Security

- Ensure any personal and sensitive documents are stored in a locked cabinet.
- Ensure portable computing devices have a physical lock to secure it.
- Destroy documents in a secure way via a shredder or authorised company.
- Take all your documents from the printer.
- Tidy away documents that contain sensitive information from your desk.
- For documents that are legally required to be kept, store in a locked room.

Digital Security

- *Dispose of any computing equipment, including mobiles in a secure way.*
- *Ensure only the required people have access to folders with sensitive data.*
- *Use encryption when sharing data that contains sensitive information.*
- *Set a password or pin code on all devices.*
- *Lock your computer / phone when left unattended.*
- *Set up 2 Factor Authentication on accounts with important information.*

Policies, Procedures and Training

- Have rules regarding document retention, storage and disposal.
- Train employees on document management and information security.
- Ensure staff are trained in data protection.

Password Security

A strong password is critical for keeping your private information secure. Here are some of the best and worst password practices :

- **Don't** use a predictable password like 123456 or qwerty123.
- **Don't** use a social login, you're handing the keys to someone else!
- **Don't** remember your passwords in a web browser.

- **Do** use a long passphrase, mixing 3 unrelated words, every character counts.
- **Do** use a unique password for each account, but especially important ones.
- **Do** ensure you change your passwords if you think it's been compromised.

Remember, never give your password when it's solicited by email, it's probably a phishing scam.