Personal & Confidential Data

User Responsibilities

These guidelines are intended to help you ensure the security of personal and confidential data.

When using the Council's data you should comply with the following guidelines.

1. All personal & confidential data should be kept in a secure filing system, or a secure ICT system.
2. All paper files shall be secured in accordance with clear desk policy.
3. All electronic data shall be secured in accordance with ICT Security policy.
4. Do not download personal data from ICT systems.
5. No personal data contained within paper files is to be taken offsite.
6. No personal data is to be copied to CD's or USB devices or any other form of removable media.
7. No personal data is to be sent by email.
8. No personal data is to be stored on laptops, Tablet's or any other mobile device unless the device is encrypted.
9. Any print outs containing personal data should be disposed of in confidential waste.
10. If you need to access personal data when offsite, do so using the secure remote access facilities.