Security Controls for All Staff

- If you are made aware of a data breach you must report it immediately.
- You must have your own username and password to access PACE systems.
- Your PACE device must have a sign in and locking mechanism.
- Your device must have antivirus, anti-malware software and firewalls with automatic updates enabled.
- Two Factor Authentication should be used for access to PACE files, cloud-based services and the database.
- Passwords should be difficult to guess, are more than 12 characters and change reminders are set on all accounts. You should never share your password.
- You should never your laptop unattended in a public setting.
- If you leave your machine you should always lock it. This would only happen at a PACE centre.
- If you are travelling with a PACE device or with hard copies of personal files they should be kept secure and, where possible, locked away out of sight. You should never leave devices or files unattended.
- When you leave the organisation your password will be reset and you will no longer have access to PACE's systems.

.