

# Computer System Access

RoS computing resources, data, information and information processes must be protected from unauthorised use, external intrusion and accidental or malicious damage. Access to equipment and software is restricted to authorised personnel only.

## Protecting Active Sessions

An unattended computer logged into an application may provide an opportunity for unauthorised access to RoS systems and information, therefore authorised users must not leave their desktop computer unattended and unlocked while logged into any application.

- PC users must [lock](#) their session (CTRL+ALT+DEL) when leaving their desk for tea breaks, lunch breaks etc. Similarly DMS workstation users must [lock](#) their workstations by selecting the [lock](#) option in their utilities menu
- At the end of the day, PC users should [shut down their PC and power it off](#)

## Other considerations

- Do not attempt to access information on the network for which you have no authorisation
- Do not attempt to access computer rooms unless authorised

**The misuse of computer facilities can in certain circumstances constitute a criminal offence under the Computer Misuse Act 1990.**

## Passwords

A user-id and password combination is a unique key for accessing RoS computing resources and information systems. It is important to choose strong passwords (see [guidance on passwords](#)) and to guard them carefully.