#Locking and shutdown

The Ministry of Justice (MoJ) has made a commitment towards sustainable IT. The intentions are:

* To reduce overall power consumption for the MoJ by switching off machines and saving energy.
* To reduce the MoJ’s overall carbon footprint.

##Shutting down a desktop computer

* Close all applications.
* Shut down the computer by clicking the ‘Start’ button at the bottom left hand corner of the screen. Next, click ‘Shut Down’.
* A pop-up box will appear with a drop-down box. Select ‘Shut Down’ and click ‘OK’. After a short delay, your computer will automatically shut down.
* Switch off your monitor screen.

##The benefits

By switching off our computers at the end of each working day, we are contributing towards being energy efficient and environmentally friendly. We are all responsible for our own Carbon Footprint. So, please switch off your PC monitor along with your desktop computer at the end of each working day. In addition, please switch off any other PC monitors if you notice they too have been left on overnight.

##Dealing with issues preventing you from switching off your computer

If there are any issues preventing you from switching off your desktop computer overnight, then please raise this with the [IT Service Desk](#Xbb07d12fea49fbb5b3e8df93e92f1bfa0e2d2a2) immediately as there could be an underlying fault that needs resolving.

If you require any further information regarding this policy, [ask for help](#contact-details).

##Locking your computer sessions

Access to most computer systems is controlled by a user name and password. If you have the correct information, you are able to ‘log in’ or ‘log on’. The user name identifies the user as a valid user of the system and the password authenticates that the user is who they say they are.

You are responsible for what you do with an MoJ system or service. You might be held responsible for any actions carried out using your user name and password. You must therefore not allow any one else to do work on any system using your user name and password. If you leave your computer logged on when you are away from it, it might be possible for sensitive information held on the computer system to be used, read, changed, printed or copied by someone not authorised to see it.

If you are leaving your computer unattended for a short period of time, ‘lock’ the computer by activating the password protected screen saver or similar ‘locking’ facility. A simple and quick way to lock a Windows computer is:

1. To LOCK - press the Windows key and L key, at the same time.
2. To UNLOCK - press the Ctrl, Alt and Delete keys, at the same time, then log in as normal.

A simple and quick way to lock a Mac computer is:

1. To LOCK - press the Ctrl, Cmd and Q keys, at the same time.
2. To UNLOCK - move the mouse or press any key, then log in as normal.

##Laptops

All MoJ laptops have hard disk encryption installed. This protects the entire contents of a laptop’s hard disk drive to prevent any data stored locally from being accessed in the event the laptop is either lost or stolen.

##Laptop incidents

Investigations into security incidents indicate that a common reason for problems is where the correct security procedures are not being followed. For example, laptops are being left logged on overnight.

This is not good security practice.

If a device is lost or stolen whilst the machine is in locked mode, the data on the machine is more vulnerable to a potential security breach.

Leaving the laptop in MoJ premises is not sufficient to guarantee the equipment’s security. Laptop losses do sometimes occur within MoJ offices. There is a greater risk of data loss when a laptop is left partially logged on overnight, so you should always fully log off the laptop at the end of your working day.

##Laptop security

* Switch off the machine completely at the end of each usage.
* Do not attach the password to the machine or keep the password with the machine.

If you need further assistance or information about this process, [ask for help](#contact-details).

##General enquiries, including theft and loss

**Technology Service Desk** - including DOM1/Quantum, and Digital & Technology Digital Service Desk. Use one of the following two methods for contacting service desk:

* Tel: 0800 917 5148
* [MoJ Service Portal](https://mojprod.service-now.com/moj_sp)

**Note:** The previous itservicedesk@justice.gov.uk and servicedesk@digital.justice.gov.uk email addresses are no longer being monitored.

**Note:** Use of the Digital & Technology Digital Service Desk Slack channel (#digitalservicedesk) is being withdrawn, and should be avoided.

**HMPPS Information & security:**

* Email: [informationmgmtsecurity@justice.gov.uk](mailto:informationmgmtsecurity@justice.gov.uk)
* Tel: 0203 334 0324

##Contacts

For any further questions relating to security, contact: [security@justice.gov.uk](mailto:security@justice.gov.uk), or for security advice, contact the [Cyber Assistance Team](mailto:CyberConsultancy@digital.justice.gov.uk).

##Feedback

If you have any questions or comments about this guidance, such as suggestions for improvements, please contact: [IT policy content](mailto:itpolicycontent@digital.justice.gov.uk).