Out with the Old

1. Before disposing of your device, make sure that all information is wiped from it so that anyone who uses it in the future cannot recover anything previously on it. To do this, reset the device to the factory default settings.

2. After you have reset the device to factory default settings ensure that the device does not automatically reconnect to your network, as you will have deleted any security software you may have installed from the device.

3. Where possible, physically destroy the device. This is the safest way of preventing anyone in the future being able to access information that was once stored on the device. Companies specialising in data destruction typically break it into pieces no larger than 6mm.

4. If you choose to have your device destroyed professionally, make sure that the company you choose meets recognised industry standards such as those published by the Asset Disposal and Information Security Alliance (ADISA).

5. If your device had a SIM card, don’t forget to remove it before you dispose, exchange or sell it.

‘Out with the Old, In with the New’

Ten tips from the Police Digital Security Centre (PDSC) to protect you and your organisation when you are replacing an electronic device.
### In with the New

1. Make sure that the seller you are buying your new device from is reputable. If you are buying a used device, ask them what steps they have taken to remove any information previously stored on it.

2. If the device is dispatched via a courier, check with the seller what checks they have made on the courier to ensure the delivery process is secure. Always ask for the delivery to be tracked and ensure that it can only be signed for by a named individual.

3. If you run a business, create an On-Boarding Policy for new devices to ensure a consistent configuration that meet your security requirements. Never assign a new device to a user or connect it to your network until this process has been completed.

4. Prevent tampering of equipment by restricting the number of people allowed to configure the initial set-up of the device. For example, a nominated administrator within your organisation who has additional rights of access to your system.

5. Keep manuals for all of the devices you use so that you can follow the manufacturers guidance when looking to dispose of them.

---

For further advice and information to protect you and your organisation from the threat of cyber-crime and fraud visit [www.policedsc.com](http://www.policedsc.com)