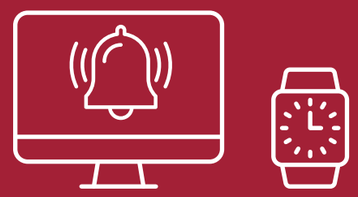
Buying and selling used devices

How to erase personal data from phones, tablets and other devices.

If you are selling, giving away, or trading in your phone, tablet, or any other device, you should **erase all of the personal data** on it. This page explains how to do this, and steps to take before you use any second-hand devices you've acquired. TVs, fitness trackers, speakers or games consoles can also contain personal information, so refer to the manufacturer's website to erase your data from these types of device*.

*A determined expert - using specialist tools - may still be able to recover the data on a device. If you really need to ensure the data can't ever be recovered, refer to the NCSC's guidance on Secure Sanitisation.

National Cyber Security Centre
a part of GCHQ



Before you erase any data

Make a backup copy of all the personal data that you want to keep, and also:

Check which accounts you access on the device (such as email, banking, shopping and social media), as well as your login details and passwords for each of these.

If you control any 'smart' devices (such as security cameras or thermostats) with your device, make sure you can do the same using a different device (such as a laptop).

If you use your device to verify other accounts (for example, by entering codes sent by text message), make sure you can do this on another device **before** you erase any data.

Erasing the data on your device

To erase all data, use your device's Erase all Content and Settings or Factory reset feature.

All your data is removed (not just messages, contacts, photos, and your browsing history, but also Wi-Fi codes, passwords, and any apps you've installed). So make sure you have a backup of anything that you want to keep.

The steps to erase data on your **specific** device may vary between models, so refer to the manufacturer's website for detailed instructions.

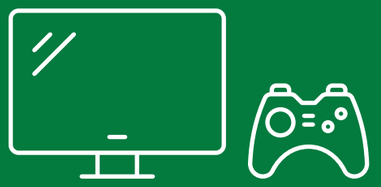
You may be given the option to keep your personal files. Do **not** choose this option if you're not keeping your phone.

Choosing a second-hand device

You don't need to buy the latest (or most expensive) device to stay safe, but if possible, avoid buying ones that are no longer supported by the manufacturer.

If a device isn't supported it won't receive security updates from the manufacturer, and without those the device is easier to hack.

Check online to see if the model you're considering can still receive updates from the manufacturer.



Before using your second-hand device

Once you've received your second-hand device, erase all the personal data on it by running a 'factory reset'. This ensures your phone is in the best possible state before you start using it.

To reset the device, you may need to refer to the manufacturer's website, as the steps to take will vary between different models.

If you're prompted to switch on automatic updates, do it. You might also want to switch on automatic backups.

Set up a screenlock using a password, fingerprint, face ID or PIN. It will help keep your phone (and the data on it) secure.