National Cyber Security Centre

Buying & selling used devices

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

If you are selling, giving away, or trading in your smartphone, tablet, or any other device, you should **erase all of the personal data** on it. This page explains how to do this*. It also suggests steps to take **before** you start using any second-hand devices you may have acquired.

Erasing personal data from devices

If you are selling, giving away, or trading in your phone or tablet (or other device), you should erase **all** of the personal data on it, so this doesn't fall into the wrong hands.

This guidance is focussed on erasing the data from phones and tablets, but you may have smart TVs, fitness trackers, speakers or games consoles that also contain personal information. Refer to the manufacturer's website to find out how to erase your data from these types of device (often called a 'factory reset').

If you've just acquired a second-hand device, we've also included some advice about what to do **before** you start using it.

*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.

Before you erase the data on your device

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

Make sure you know 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 use your device to control any 'smart' devices (such as security cameras or thermostats), make sure you're able to manage them using a different device, before you erase your data.

If you use your device to verify online accounts (for example, by confirming SMS codes), make sure you can do this on another device before you erase the data on the device that you're selling/giving away.

Erasing the data on your device

To ensure sure your data is completely erased, use your device's **Erase all Content and Settings** or **Factory reset** feature:

This will remove all your personal data (such as messages, contacts, photos, browsing history, 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 when erasing your data; do not choose this option if you're not keeping your device.

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 find if the specific 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 your second-hand 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 you should do this. 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.