

GUIDANCE

Buying and selling second-hand devices

How to erase the personal data from your phone, tablets, and other devices (and why it's important when you're buying and selling them).

Our devices – and especially our smartphones – contain more work, personal and financial data than ever before. If you are selling, giving away, or trading in your smartphone (or other device), you should erase all of this personal data so it doesn't fall into the wrong hands. This page explains how to do this, and the important steps to take beforehand.

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

Note

This guidance is focussed on erasing the data on smartphones and tablets, but you may have other electronic devices (such as smart TVs, fitness trackers, speakers or games consoles) that will also contain personal information.

If you're selling devices like this, refer to the manufacturer's website (or search online) to find out how to erase your data from these devices – often called a 'factory reset'.

Before you erase the data on your device

There are a number of things you need to check before you erase the data on your device.

1. Make sure you have a backup copy of all the personal data that you want to keep. The instructions below will remove **all** of your personal data that's stored on your device.
2. If you use your device to access online services (such as banking, shopping, email or social media), you might be logging into these services **without** entering your password each time. If this is the case, make sure you know which accounts you access (and the logins and passwords for each of these accounts) **before** you erase your data.
3. If you use your device to control any of your 'smart' devices around the house (such as security cameras or thermostats), you'll no longer be able to manage them using your phone. Again, make sure you're able to manage them using a different device, before you erase your data.
4. If you use your device to verify your online accounts (for example, by confirming SMS codes), you'll need to make sure this works on another device. Make sure you do this (and check that it works) before you erase the data on the device that you're selling/giving away.

Erasing the data on your device

The best way to make sure that your data is completely erased* is to use your phone's **Erase all Content and Settings** or **Factory reset** features. The exact name of the feature will depend on which type of device you have. Using the feature will remove **all** your personal data from your device (including messages, contacts, photographs, browsing history, Wi-Fi codes, passwords, and any apps you've installed), so make sure you have a backup of all the data that you want to keep.

To delete all the data on your *specific* device, you may need to refer to the manufacturer's website, as the steps to take will vary between different models. To get you started, we've included links to the major phone and computer models.

- [Reset your Android device to factory settings](#)
- [Erase your iPhone, iPad or iPod touch](#)
- [Reset your Chromebook to factory settings](#)
- [Start afresh with a clean installation of Windows 11](#)
- [Restore your Mac to factory settings](#)

You may be given the option to keep your personal files when erasing your data. Make sure you **don't** choose this option if you're selling, trading in, or giving your device away.

Choosing a second-hand device

You don't need to buy the latest (or most expensive) model to stay safe, but if possible, **avoid** buying phones that are no longer supported by the manufacturer (or whose support period will end soon). If you buy a phone that is no longer supported:

- it **won't** receive updates that contain new features and performance improvements
- it **won't** receive the security updates from the manufacturer (and without these your phone is easier to hack)

You can check online to find if the specific model you're considering can still receive updates from the manufacturer. Here are the details for iPhone, Chrome, and Pixel/Nexus devices.

- [Supported iPhone models](#)
- [Chrome OS \(e.g. Chromebooks\)](#)
- [Pixel devices](#)

If you have another type Android device (such as those manufactured by Samsung or Huawei), you'll have to [check with the manufacturer](#).

If you're buying a second-hand device online, we encourage you to read the NCSC's guide to [shopping online securely](#).

Before using your second-hand device

Once you've received your second-hand device, it's a good idea to erase all the personal data on it, or perform a 'factory reset' (the exact name of this feature will depend on which type of device you have). This reset will delete the previous owner's data, (including their messages, contacts, photographs, browsing history, Wi-Fi codes, passwords, and any apps they've installed). It will also ensure 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. To get you started, we've included links to the major phone and computer makes.

- [Reset your Android device to factory settings](#)
- [Erase your iPhone, iPad or iPod touch](#)
- [Reset your Chromebook to factory settings](#)
- [Start afresh with a clean installation of Windows 11](#)
- [How to restore MacOS](#)

If you're prompted to switch on automatic updates (or to set up a screenlock, password, fingerprint or PIN) you should do this, as they will help keep your phone (and the data on it) secure. You might also want to [switch on automatic backups](#), so you've one less thing to worry about the next time you switch devices.

***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 our guidance on [secure sanitisation](#).**

PUBLISHED

28 December 2020

REVIEWED

7 November 2022

VERSION

1.0

WRITTEN FOR

[Individuals & families](#)

[Self employed & sole traders](#)