What is biometric data?

KS3 KS4 Ages 11-16 ⏰ 4 min read

Every time you unlock your phone with your face, pass through an airport e-gate, or get your fingerprint scanned at a theme park, you're interacting with biometric technology. Biometric data is any physical or behavioural characteristic that uniquely identifies a person — and it's increasingly woven into the infrastructure of daily life.

What counts as biometric data?

The most common types are fingerprints, facial geometry, iris patterns, and voice prints. But the category is broader than most people realise. Your **gait** (the way you walk) is sufficiently unique to identify you on CCTV. Your **typing rhythm** — the specific pattern of pauses between keystrokes — can identify you even without knowing your password. Heart rate patterns, ear shape, and vein patterns in the hand have all been used as identifiers. If it's a measurable physical or behavioural trait unique to you, it's potentially biometric.

🔑 A password is like a key — if someone gets a copy, they can use it, and you can change it if it's stolen. Biometric data is more like the shape of your hand itself. It can't be easily copied and it's always with you — which makes it convenient. But if it's ever compromised or misused, you can't change it. You can't get a new face the way you can reset a password.

Why is it increasingly used?

Because it's convenient and hard to forge. A face or a fingerprint can't be forgotten, lost, or easily shared in the way a password can. For high-security applications — border control, banking, unlocking devices — biometrics offer a strong guarantee that the person is who they claim to be. The technology has also become cheap enough to put in consumer devices.

What are the risks?

The risks are significant. Unlike passwords, biometric data is permanent — if a database of facial recognition data is breached, you can't issue everyone a new face. It's also inherently personal: collecting someone's biometrics is collecting something

intimate and inalienable from their body. Facial recognition in particular has attracted controversy because it can be used for mass surveillance in public spaces without people's knowledge or consent — which is why several cities have banned its use by police. There are also accuracy concerns: some facial recognition systems have shown higher error rates for people with darker skin, raising serious concerns about discriminatory policing.

In the UK and EU, biometric data is classified as a special category of personal data under data protection law, meaning it requires explicit consent and tighter controls to collect and use. Whether those controls are sufficient as the technology becomes more pervasive is one of the defining privacy debates of our time.