

Small business IT | Easy | 2 min read

What to do when a work laptop is lost or stolen

It happens to many businesses. Acting quickly protects your data and your customers. This is general information, not legal advice.

Straight away

1. **Tell the person in charge**, and make a note of when and where it was lost.
2. If stolen, **report it to the police** and get a crime reference number, which is useful for insurance.
3. From another device, change the password of the account used on the laptop, including email, and the password manager.
4. **Sign out all sessions** and remove the device from your cloud accounts, for example in Microsoft 365 or Google account settings.
5. Use "Find my device" for Windows or Mac to locate, lock, or wipe it, if you set it up beforehand.
6. Contact your IT provider if you have one.

Think about what was on it

- Was the drive **encrypted** with BitLocker or FileVault? If so, risk is much lower.
- Was there customer or staff data stored on it?
- Were passwords saved in the browser, or was the laptop signed in to payment or banking systems?
- Were files stored only on the laptop? Restore them from your backup.

Personal data

If personal data may have been exposed, consider whether you must report it to the ICO. Under UK GDPR this is usually within 72 hours of becoming aware, if there is a risk to individuals. The ICO website has guidance and a self-assessment. Tell affected people if there is a high risk to them.

Afterwards

- Update your equipment register.
- Replace the device and set it up with encryption and a screen lock.
- Tell your insurer, and check your policy for cover.
- Review how it happened and how to prevent it.

When to get more help

Get help if the laptop held unencrypted customer data, if it was signed in to banking or payment tools, or if you do not know what was on it.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.