Lost or stolen device playbook

Edition 16 November 2026. Free to copy and adapt under CC BY 4.0. Fields in [square brackets] are for you to fill in.

When to use this playbook

Use this playbook when a laptop, phone, tablet, removable drive or paper record that holds business data is lost, stolen or misplaced.

Before you start: prerequisites

Complete these before an incident, as part of planning.

- A current asset list says which devices hold which data.
- Devices are encrypted, and the list shows which ones are.
- Remote lock and wipe is set up and tested for phones and laptops.
- Staff know to report a loss at once, at any hour.

Workflow

Work in this order. Record each step and its time in the incident log.

1. Record when and where the loss was noticed, when it was last seen, and who had it.
2. Lock or wipe the device remotely and revoke its sessions, tokens and certificates.
3. Reset passwords for accounts that were signed in on the device.
4. Find out what was on the device and whether it was encrypted and locked.
5. Check logs for sign-in attempts from the device after the loss.
6. If it may have been stolen, report to the police and record the report number.
7. Decide whether this is a reportable breach, using the encryption facts.

Decision points

Stop at each of these and record the decision, the decider and the time.

Decision	Who decides	Information needed
Was the data protected by encryption?	Technical lead	Device encryption status and key handling
Is it a reportable breach?	Privacy lead, legal	Data types, people affected, rules in section 10
Wipe now or wait?	Technical lead	Chance of recovery versus risk of access

Notices to check

Open section 10 of the plan and confirm whether any of these start a notice clock.

- Under HIPAA, only unsecured protected health information triggers breach notice; the rule defines it by whether the information was rendered unusable, unreadable or indecipherable.

- Under GDPR Article 34, communication to individuals is not required if the data was protected by measures such as encryption that made it unintelligible to unauthorized people.

Exit criteria and follow-up

Close the playbook only when all of these are true.

- The device is recovered or wiped, and sessions revoked.
- The reportability decision is recorded with reasons.
- The asset list is corrected.