06. Incident response and breach reporting plan

> **Template.** Part of the open-source AI App Policy Kit, version 1.0. Replace everything in [square brackets], delete what does not apply, and have the person who runs the business approve it. A starting point, not legal advice.

Business	[Business name]
Document owner	[Name and role]
Approved by, and date	[Name], [date]
Next review	[Date, at most 12 months on]

Why this matters

When something goes wrong, the first hours decide how bad it gets. UK GDPR gives you 72 hours from becoming aware of a personal data breach to report it to the ICO, if it is likely to put people at risk. A plan written beforehand means nobody has to work it out under pressure.

Who it covers

Everyone at [Business name]. Anyone may raise an incident. The incident lead runs it.

What counts as an incident

- Someone got in who should not have, or may have: a stolen login, a leaked key, an unknown admin account.
- Personal data was lost, sent to the wrong person, published or changed by mistake.
- The app is down or data is missing.
- An AI feature revealed one customer's data to another, was tricked into doing something it should not, or gave harmful advice.
- A supplier tells you they had a breach.
- A lost or stolen laptop or phone.

Contacts

Role	Name	Phone	Backup
Incident lead	[Name]	[Number]	[Name, number]
Technical lead	[Name or supplier]	[ ]	[ ]
Decides on reporting to the ICO	[Director's name]	[ ]	[ ]
Cyber insurance	[Insurer, policy number]	[Claims line]	
Hosting and AI suppliers	[Support contacts]	[ ]	

The steps

1. **Raise it at once.** Tell the incident lead by phone, whatever the hour. Note the time you became aware: the 72 hours start here.

2. **Contain.** Revoke the leaked key, disable the account, take the affected feature offline. Do not delete evidence: keep logs, and take a copy of the affected system if you can.
3. **Assess.** What happened, to which data, about how many people, and is it still going on? Write down what you know and what you do not.
4. **Decide on reporting, within 72 hours.**
    - *Is personal data involved?* If not, no ICO report is due.
    - *Is a risk to people likely* (fraud, identity theft, distress, discrimination, financial loss)? If yes, report to the ICO within 72 hours of becoming aware, even with incomplete facts. You can add detail later.
    - *Is the risk high?* Then also tell the people affected without undue delay, in plain words: what happened, what it means for them, what you are doing and what they should do.
    - Record the decision and the reasons either way.
5. **Tell others who must know.** The insurer, as the policy requires. Business customers whose data you process, as the contract requires. Action Fraud if a crime was committed. The bank if payment details are involved.
6. **Recover.** Fix the cause, restore from backup if needed (document 07), change every secret that could have been exposed and watch closely for a repeat.
7. **Review within two weeks.** What happened, what worked, what did not and what changes. Assign each action to a named person with a date.

Incident log

Record every incident, reported to the ICO or not.

Date and time aware	What happened	Data and people affected	Reported to ICO? (date, reference, or reason not)	People told?	Cause	Actions and owner
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

Checklist

- ☐ The contacts table is filled in and was checked in the last 6 months.
- ☐ A printed copy of this plan exists, in case the systems are down.
- ☐ The team walked through a practice incident in the last 12 months.
- ☐ Every incident in the log has a review and closed actions.

References

- ICO, *Personal data breaches: a guide* and the ICO's breach reporting service.
- NCSC, *Small Business Guide: Response and Recovery*.

AI App Policy Kit, version 1.0. © 2026 PugliseWeb LTD, licensed under CC BY 4.0: use it, change it and share it, with credit. The whole kit, and a free

Software Health Check of your app against it: https://www.puglieseweb.com/ai-policy-kit