AI incident response one-pager

For the day an AI tool leaks, invents, or misfires: who does what, in what order.
Fill it in calm; use it in a hurry.

01 Roles

Incident owner (name, phone)

Deputy (name, phone)

DPO / data protection adviser

Regulatory contact decision-maker

02 First hour

- [ ] Stop the tool or workflow involved (the tested stop switch)
- [ ] Preserve the logs: what went in, what came out, who saw it
- [ ] Establish scope: whose data, which outputs, sent where
- [ ] Notify the incident owner; nobody else improvises comms

03 First day

- [ ] Personal-data breach assessment: is ICO notification in play (72h clock)?
- [ ] Affected clients identified; correction plan for any wrong output that reached them
- [ ] Vendor engaged in writing where their system was involved

Notes / timeline

04 After

- [ ] Written incident record completed (what, why, fix)
- [ ] The control that would have prevented it, added

- [ ] Policy / register / training updated the same week