AI Risk Assessment Worksheet

One assessment per use case — not per tool

1. Define the use

What task will AI perform?

2. Identify the information

What data enters and leaves? Classify it: public, internal, confidential, personal, special category.

3. Identify people affected

Customers, staff, applicants, suppliers or the public?

4. Assess consequences

What happens if it is wrong, unavailable, biased or breached?

5. Assess the supplier

Terms, security, data use and resilience.

6. Define controls

Human review points, access limits, anonymisation, logging, testing.

7. Assign an owner

Name the accountable role.

8. Approve or reject

Approved / restricted / pilot / prohibited — with reasons.

9. Monitor

Review incidents, changes and performance at a defined interval.

Risk level

- ☐ LOW — approved tool, basic rules, light review
- ☐ MODERATE — named owner, defined human review, source checking, records
- ☐ HIGH — full assessment, strongest supplier scrutiny, qualified human review, DPIA where personal data is involved, senior sign-off

Owner: ______________________________

Review date: ______________________