aptem.
Intelligent technology®

AI use and governance charter

Starter template

A starting point for your organisation to adopt and adapt for its own AI policy.

Provided by Aptem

Version: 1.0

Owner: [Charter Owner]

Status: [Draft / Active]

Date: [Day Month Year]

Audience: customer-facing starter template

aptem.
Intelligent technology®

Contents

aptem.
Intelligent technology®

How to use this template

This document is a starting point. It is not a finished policy. You should edit it, cut what is not relevant to your organisation, and add anything that is missing for your context.

What to do first

1. Replace every placeholder in square brackets (for example, [Organisation], [Charter Owner], [senior leadership / board]) with your own names and links.
2. Decide who owns this charter. The Charter Owner is the single named individual responsible for keeping it current and reporting on it to your leadership.
3. Decide your audience. This charter is normally a public-facing document that any employee, contractor, or supplier can read.
4. Decide your sign-off route. Most organisations have this approved by an executive or board-level forum.

What to do next

- Pair this charter with an AI register, a tool approval process, an AI Suitability and Impact Assessment (AISIA) template, and a Data Protection Impact Assessment (DPIA) template. The charter sets the rules; the register and assessments operate them day to day.
- Set a review date. Annual review is the minimum. Many organisations also trigger review on any material regulatory or technological change.
- Make staff training a hard requirement, not a recommendation. Section 9 sets out a simple three-level model.

A note on standards

The structure of this charter is aligned to ISO/IEC 42001 (AI Management Systems) and ISO/IEC 27001 (Information Security Management Systems). You do not need to be pursuing certification for this charter to work. If you are, the structure should hold up against the relevant Annex A controls without needing to be rewritten.

aptem.
Intelligent technology®

1. Purpose

This charter sets out [Organisation]'s framework for the responsible, ethical, and secure use of Artificial Intelligence (AI) across all operations, products, and partnerships.

It ensures that AI adoption and development align with:

- UK GDPR and the Data Protection Act 2018
- The principles set out in the UK Government's AI policy framework
- EU AI Act principles, where relevant to [Organisation]'s operations
- ISO/IEC 42001 (AI Management Systems) and ISO/IEC 27001 (Information Security Management Systems), where [Organisation] is pursuing certification or alignment

This charter complements [Organisation]'s supplier management policy. Where AI-related suppliers are involved, both policies apply.

aptem.
Intelligent technology®

2. Scope

This charter applies to:

- All [Organisation] employees, contractors, and third parties who develop, procure, or use AI.
- All AI systems, internal or external, used in operations, decision-making, service delivery, or customer-facing functions.
- All suppliers providing AI-based services or tools.

aptem.
Intelligent technology®

3. What we mean by AI

Artificial Intelligence (AI) refers to systems and technologies capable of performing tasks that would typically require human intelligence or effort. This includes reasoning, pattern recognition, prediction, decision-making, and language understanding.

Common forms of AI include:

Type	Description	Examples
Machine learning (ML)	Systems that learn patterns from data and improve performance over time.	Recommendation engines, spam filters, credit scoring.
Natural language processing (NLP)	Systems that process or generate human language.	Chatbots, transcription tools, large language models.
Computer vision	Systems that interpret images or video.	Image recognition, document scanning, facial detection.
Predictive analytics	AI models that forecast trends or behaviours based on data.	Progression prediction, demand forecasting.
Generative AI	Models that create new content such as text, code, or images.	ChatGPT, Claude, Copilot, image generators.

How AI shows up in your work

AI may be used:

- Directly by employees (for example, drafting tools, code assistants, transcription).
- Indirectly through suppliers or systems that include AI features (for example, analytics dashboards, document scanning, chatbots).
- In internal automation or product development.

aptem.
Intelligent technology®

Shadow AI

Using unapproved AI tools or features outside official channels is treated as a breach of this charter. Employees must seek review and approval before introducing or integrating any new AI tool or service. This includes free tools, browser plugins, and AI features inside otherwise approved software.

aptem.
Intelligent technology®

4. Guiding principles

Every AI use case at [Organisation] must uphold the following principles.

Fairness and non-discrimination

AI must be designed and used in ways that minimise bias and avoid disadvantaging individuals or groups.

Transparency and explainability

Decisions made or supported by AI must be traceable and explainable. People affected by an AI-driven outcome should be able to understand, in plain terms, how the outcome was reached.

Human oversight and accountability

A named person is accountable for every AI system in use. Humans must be able to override AI-driven outcomes and individuals must have a route to appeal.

Data protection and lawful basis

Personal data used in AI systems must have a lawful basis under UK GDPR. Data minimisation, purpose limitation, and retention limits apply.

Purpose limitation

AI tools are used only for the purpose for which they were approved. Reuse of an approved tool for a new purpose requires a fresh assessment.

Security

All AI tools must comply with [Organisation]'s information security and data protection standards. Suppliers must meet the data security requirements set out in the supplier management policy.

aptem.
Intelligent technology®

5. Roles and accountability

Role	Responsibility
Charter Owner	Owns this charter. Maintains the AI register. Reports to [senior leadership / board] at least annually on AI use, risks, and incidents.
AI Owner (per system)	Named individual for each AI system in use. Responsible for lifecycle documentation, ongoing monitoring, incident response, and ensuring the system continues to meet the charter.
Data Protection Officer / Compliance lead	Ensures legal alignment. Oversees AI Suitability and Impact Assessments (AISIAs) and Data Protection Impact Assessments (DPIAs). Monitors supplier conformance and reports on incidents.
All employees and contractors	Use only approved AI tools. Follow this charter. Complete required training. Raise concerns through the route in Section 10.

aptem.
Intelligent technology®

6. Permitted and prohibited uses

6.1 Permitted uses

Subject to the appropriate assessment and approval being in place, AI may be used for:

- Productivity and content generation (for example, summarisation, drafting, code assistance).
- Research, data analysis, and innovation.
- Product features and customer support, with documented human oversight.
- Use of customer or business data, but only as approved under a specific AISIA.

6.2 Prohibited uses

The following are not permitted under any circumstance.

1. Training or fine-tuning AI models using personal, customer-provided, or otherwise protected data, unless exceptional written approval is in place. Approval is considered only where anonymised or synthetic data cannot reasonably achieve the same outcome and where strict technical and contractual controls apply.
2. Inputting protected data into public AI services where that data will be used to train the supplier's models. This includes free-tier consumer AI services without enterprise data-handling controls.
3. Surveillance, behaviour scoring, or any use that contravenes UK law, regulation, or [Organisation]'s policies.
4. Generating content that is discriminatory, deceptive, or designed to mislead.
5. Any AI use that removes a person's right to a human review or appeal of an outcome that affects them.

Publicly available information (for example, government policy documents, public company data) is not restricted by these rules.

aptem.
Intelligent technology®

7. Risk classification

Every AI system or tool must be risk-classified before procurement or deployment. Classification determines the controls and the review frequency that apply.

Baseline controls (all AI systems)

- AISIA and DPIA completed before deployment.
- Registered in [Organisation]'s AI register.
- Data mapping, minimisation, and lawful basis confirmed.
- Security and privacy testing carried out.
- Human oversight points documented.
- Logging, traceability, and monitoring plans in place.
- Supplier evidence of compliance held on file (for external tools).
- Reviewed at least annually, or sooner on any material change.

Risk tiers

Tier	What it covers and typical examples	Controls (additional to baseline)	Review
Low risk	AI that has little or no effect on individuals or consequential decisions. Examples: code assistants, summarisation, grammar and translation tools, internal search over public information, marketing content drafts.	Confirm AISIA and DPIA complete. Staff trained on responsible use and data entry hygiene. Clear disclosure to users when they are interacting with AI. Label synthetic content (text, image, video).	Annual
High risk	AI that influences outcomes for individuals or processes	All low-risk controls, plus:	Quarterly

	personal data with potential impact on rights or eligibility. Examples: models predicting outcomes for service users, automated applicant scoring, compliance automation, third-party analytics processing personal data.	Formal risk management file (hazards, mitigations, residual risk). Data governance documentation (provenance, quality, bias tests). Defined human oversight model: who reviews, when, and how to override. Accuracy, robustness, and security testing. Sign-off by [senior leadership / board].	
Prohibited	AI that breaches law, regulation, or this charter. Examples: training on protected data without exceptional approval, surveillance or behaviour scoring, discriminatory or deceptive outputs, AI use that removes a person's right to human review.	Not permitted under any circumstance.	Not applicable

Ethics and legal checklist

Before approving an AI use case, the AI Owner must confirm each of:

- Respects human oversight and autonomy.
- Demonstrates fairness and active bias mitigation.
- Maintains transparency and explainability for users.
- Processes data only within the lawful purpose and contract.
- Complies with [Organisation]'s policies, including the supplier management policy.

aptem.
Intelligent technology®

8. Approval process for new AI tools

Use this six-step process for every new AI tool, model, or significant change to an existing one.

1. Define the use case and appoint an AI Owner. Document the business purpose, the data involved, and who is accountable.
2. Complete an AISIA and a DPIA. Cover purpose, lawful basis, data flows, bias risks, and human oversight.
3. Carry out a security and supplier review. Check the supplier's compliance position, data residency, sub-processors, and any AI-specific contract clauses.
4. Assign a risk tier. Attach the artefacts required for that tier.
5. Obtain sign-off from the Charter Owner. High-risk cases require additional sign-off from [senior leadership / board].
6. Register in [Organisation]'s AI register. Enable logging, monitoring, and the audit trail.

Material changes to the model, data, purpose, or supplier invalidate the prior approval and require re-assessment.

aptem.
Intelligent technology®

9. Training and competence

Every employee at [Organisation] is required to complete AI training appropriate to their role.

Level	Audience	Requirement
Level 1: General awareness	All employees and contractors.	Annual training on responsible AI use and data protection.
Level 2: Practitioner	Developers, analysts, product staff, and anyone designing or operating AI systems.	Targeted training on AI design, bias mitigation, prompt practice, and lifecycle management.
Level 3: Owner	Senior staff responsible for AI governance, including the Charter Owner and individual AI Owners.	Advanced training aligned with the relevant standards and supplier oversight requirements.

aptem.
Intelligent technology®

10. Monitoring, incidents and review

Monitoring

The Charter Owner, supported by the Compliance lead, maintains an AI register and an AI risk dashboard. Both are reviewed against the incident log on a regular basis.

Incidents

An AI incident is anything that suggests an AI system is failing to meet this charter. Examples include:

- Unexpected bias or unfair outcomes.
- Personal or protected data exposure.
- Supplier failure or material change.
- Unexpected or undocumented system behaviour.
- Use of AI tools outside the approval process (Shadow AI).

All AI-related incidents must be reported within 48 hours via [Organisation]'s incident reporting route. The Charter Owner is informed for every incident at high-risk or above. Serious incidents are escalated to [senior leadership / board].

Review

This charter is reviewed annually, or sooner on any material regulatory or technological change.

aptem.
Intelligent technology®

11. Related policies and references

Used together, the documents below operate the charter day to day. Replace each with a link to your own version, or remove anything that does not apply to [Organisation].

- [Organisation] supplier management policy
- [Organisation] information security policy
- [Organisation] data protection policy
- [Organisation] incident reporting procedure
- AISIA template
- DPIA template
- [Organisation] AI register

External standards and frameworks

- UK GDPR and Data Protection Act 2018
- UK Government AI policy framework
- EU AI Act (where applicable)
- ISO/IEC 42001 Artificial Intelligence Management Systems
- ISO/IEC 27001 Information Security Management Systems