

Safe AI Adoption

OUR DATA PROTECTION STANDARDS · HOW WE WORK · EVERY ENGAGEMENT, EVERY SECTOR

In any business, data protection is not a hurdle to clear before adopting AI. It is the design principle that determines which adoption is possible. Every engagement is built on the five standards below.

THE PRIME RULE — NON-NEGOTIABLE

No personal or commercially sensitive data ever enters a public AI tool. Not customer or employee names, not financial or health details, not information that could identify an individual or expose confidential business matters.

Many businesses hold special category data — health, HR, financial and safeguarding information attracting the highest protection under UK GDPR. Even “anonymised” detail can identify a person in a small team or customer base, so our workflows ensure identification only ever happens inside your own systems, by your own staff.

— The Five Standards

1 Data minimisation by design

AI works on structures, templates and de-identified content — never on personal data. It drafts the framework and the language; your qualified people add the specifics. The result: the full time saving, with zero personal-data exposure.

2 Enterprise-grade tools, under contract

Only business-tier AI services with signed data processing agreements, contractual commitments that inputs never train models, appropriate UK/EU data handling and audit logging. Consumer free-tier tools are excluded by policy.

3 Governance before deployment

A Data Protection Impact Assessment framework before anything goes live — the ICO expects a DPIA wherever innovative technology meets personal data. Privacy notices reviewed and a staff AI acceptable-use policy in place. Where you have a DPO, we design; they validate.

4 Human judgement, always

AI drafts; professionals decide. Nothing AI-assisted reaches a customer, a regulator or a formal record without qualified review and sign-off. AI supports the expertise in the business; it never substitutes for it.

5 Capability, not just compliance

Policy without training fails. Staff are trained in safe, confident use — what may go into a tool, what never may, and how to review output critically — so safe practice becomes culture, not a document in a drawer.

— Aligned to the Frameworks Businesses Are Held To

UK GDPR & DPA 2018

Including Article 9 special category data and the enhanced protection personal data attracts.

ICO EXPECTATIONS

DPIA-led adoption where new technology meets personal data; documented, defensible decision-making.

SECTOR STANDARDS

Tool selection benchmarked to your sector's regulators and guidance — for example, DfE standards and KCSIE in education.

AUDIT & INSPECTION

A governance record that stands as evidence for clients, insurers, regulators and inspection.

Scope of our role. We design and implement AI workflows aligned with ICO guidance and the standards of your sector, and prepare the supporting governance documentation. This is operational advisory, not legal advice: formal DPIA approval and data protection accountability remain with your business as data controller, supported by its DPO or legal adviser — with whom we work openly and gladly.

It starts with a conversation — free, informal, no obligation.

calendly.com/mark-marklindleyconsultants · mark@marklindleyconsultants.co.uk · marklindleyconsultants.co.uk

SAFE AI AD

MARK LINDLE