TRAINING CHECKLIST

This checklist is designed to help organisations plan, deliver and monitor effective data protection training for all staff. It supports compliance with data protection law and promotes a culture of privacy awareness across the organisation. Use it to confirm that all employees receive the right level of training — from general awareness for all staff to specialist training for those handling higher-risk processing activities (please note that this checklist doesn't relate to Data Protection Officers as more role specific and specialist training is required).

Data protection training is not a one size fits all approach. Depending on the amount and types of personal information accessible in a person's role and the level of responsibility, training should be tailored to reflect the associated risk(s) of such. We expect that staff receive the relevant training which is refreshed on an appropriate frequency – so that knowledge is kept up-to-date, the frequency of training is to be assessed and noted internally. Consider the most suitable format for delivery, whether that be face-to-face, online, e-learning etc. Consider when this training will be delivered to new starters, i.e. during the induction process and how you are assessing competency levels of those taking the training. The level of training may need to be reconsidered during a change of role, if applicable.

The checklist can also help demonstrate accountability by providing a record of how training needs are identified, implemented, and reviewed.

1. TRAINING GOVERNANCE & PLANNING

□ Training lead/owner identified and accountable for programme.

□ Training plan aligns with organisational data protection risks and roles.

□ Training required before or soon after staff access personal data.

□ Refresher training scheduled (annually or biennially).

□ Records of all training maintained (attendance, date, version, assessment).

□ Training content reviewed regularly and updated for changes in law/processing.

2. GENERAL AWARENESS TRAINING (ALL STAFF)

□ Covers relevant data protection law(s) applicable to the organisation.

□ Explains data protection principles and practical application.

□ Defines personal data and special category data.

□ Explains data subject rights and internal handling procedures.

□ Covers breach identification and internal reporting procedure.

□ Includes good practice: phishing, secure disposal, remote working, data sharing.

□ References organisation-specific policies, contacts, and DPO details.

3. ROLE/SPECIALIST TRAINING

□ Roles needing enhanced/specialist training identified (e.g., HR, IT, Marketing).

□ Training covers role-specific processing and risks.

□ Covers lawful basis for processing and additional safeguards for special data.

□ Includes DPIA, risk assessment and privacy by design processes.

□ Covers data sharing, contracts, international transfers, and security controls.

□ Covers retention, destruction, and archiving for relevant data types.

□ Includes governance, oversight, and sector-specific compliance requirements.

□ Competency assessed after training (test or scenario).

□ Training reassessed upon change of role or new processing activity.

4. DELIVERY & RECORDS

□ Training format suitable for audience (e-learning, workshop, blended).

□ Provider tailors training to organisation's processing and law.

□ Training includes case studies and real-world scenarios.

□ Interactive elements included (quizzes, breach simulations, role-play).

□ Refresher and update briefings provided after regulatory or system changes.

□ Training accessible and inclusive for all staff groups.

□ Version control and training material archive maintained.

5. MONITORING & REVIEW

□ Training log/database maintained with dates, versions, outcomes.

□ Completion and assessment rates monitored and reported.

□ Feedback from participants gathered and analysed.

□ Training effectiveness measured against incidents and audits.

□ Content reviewed and refreshed following law, process or incident changes.

□ Gaps or deficiencies escalated and addressed promptly.

6. INTEGRATION WITH WIDER GOVERNANCE

□ Training aligned with policies (data protection, breach, retention, DPIA).

□ Roles and responsibilities clearly defined (DPO, leads, managers).

□ Training aligned with information security and cyber-security programmes.

□ Staff understand how their role interacts with data protection obligations.

□ Awareness culture promoted through leadership and communications.

□ Training linked to incident response and continuous improvement processes.

7. WHEN GENERAL TRAINING MAY NOT SUFFICE

□ High-risk or large-scale processing identified and specialist training provided.

□ Staff handling profiling, AI, or automated decision-making receive additional training.

□ Procurement and vendor management teams trained on data processing agreements.

□ IT and development staff trained on secure design and technical safeguards.

□ Remote/hybrid workers receive specific guidance on secure data handling.

□ Sector-specific or regulated functions receive tailored compliance training.

□ Training requirements reviewed for new systems or processing changes.