

01 MAP AND CONTROL AI USE • Keep a live AI register: tool, user, purpose and data used. • Confirm approved AI tools and set “do not upload” rules for public or unapproved AI tools. • Route new or unapproved tools through legal, privacy, IT/security or AI governance review.	02 REVIEW TOOLS, CONTRACTS AND DATA • Add AI procurement checks: purpose, training data, outputs, licences and indemnities. • Review contracts for AI-related IP, confidentiality, data rights and contractor terms. • Document AI data provenance: source, permitted use and approval	03 EMBED HUMAN REVIEW AND TRAINING • Add AI review checkpoints from project set-up to client delivery. • Define when AI outputs need human review for accuracy, fairness, privacy or IP risk. • Provide baseline AI training for all staff, plus deeper modules for research, legal, data and client teams.
---	--	---

FOR COMPLIANCE TEAMS Maintain an AI register, clarify approved tools, and review relevant policies, contracts and vendor terms.	FOR RESEARCH TEAMS Build AI checks into research workflows, document data use and review outputs before delivery.	FOR SENIOR STAKEHOLDERS Set AI risk appetite, fund approved tools and training, and create cross-functional oversight.
---	---	--

Kay Firth-Butterfield CEO, Good Tech Advisory LLC	• Used songwriter example to show how AI training can raise questions about protected work, consent, compensation and accountability. • Framed AI compliance as an organisation-wide governance issue, including for small businesses. • Emphasised practical controls: map AI use, manage shadow AI, train staff and review regularly.
Barry Scannell Partner, William Fry	• Explained that AI and IP law is still developing, with limited definitive case law across jurisdictions. • Warned that free AI tools can expose confidential, privileged, source code or trade secret material. • Recommended core safeguards: AI policies, staff training and clearer contracts covering IP and confidential information.
Ravinder Roopra CPO/DPO Head of Privacy, Data, Cyber and AI, Kantar	• Outlined AI and IP risks across the research process, from data inputs to outputs. • Stressed clear documentation of data sources, model inputs, approvals and data use. • Shared Kantar’s risk approach: model cards, transparency, explainability, checkpoints and targeted training.

KEY POINTS TO SHARE INTERNALLY AI innovation and IP protection go hand in hand. Document data sources, confirm approvals, review contracts and vendor terms, apply governance controls and train staff.	CLOSING SUMMARY Responsible AI innovation depends on clear data controls, sound contracts, governance, human oversight and staff training.
---	--