AI CHECKLIST

Area	Checklist Item	☑
Tool-by-Tool Compliance	List all AI tools in use (ChatGPT, Copilot, Gemini, Otter.ai, Fireflies, Read.ai, Grammarly, etc.)	☐
	Check each tool against NZ Privacy Act & Australian Privacy Principles	☐
	Confirm vendor certifications (ISO, SOC2, NDIS compliance)	☐
	Identify high-risk tools (meeting transcription, generative text)	☐
	Document mitigation actions (restrict sensitive use, anonymise data, review contracts)	☐
Risk Register	Maintain a live register of AI risks	☐
	Categorise risks: Privacy, Cybersecurity, Reputation, Equity	☐
	Rate likelihood and impact (Low/Medium/High)	☐
	Assign responsibility for each risk	☐
	Review monthly; colour-code (Red/Amber/Green)	☐
Vendor Evaluation	Create a vendor matrix comparing providers (Microsoft, OpenAI, Google, Otter.ai, Fireflies, etc.)	☐
	Assess transparency of data use and storage	☐
	Check cultural safety alignment (Te Tiriti, Māori data sovereignty, equity commitments)	☐
	Review contractual protections (data ownership, breach response)	☐
	Score vendors 1–5 for compliance, transparency, and cultural safety	☐
Policy & Training	Update organisational policies to cover AI use	☐
	Train staff on safe AI practices (no sensitive data in prompts)	☐
	Provide board/staff with compliance matrices and risk registers	☐
	Embed equity, dignity, and cultural safety in AI governance	☐
	Review policies quarterly to stay audit-ready	☐
	Re-evaluate compliance fit quarterly	☐
	Use Google Search Console/analytics to track visibility of AI-related content	☐
	Report AI governance status to the board regularly	☐
	Ensure defensibility: every decision backed by documentation	☐