The Institution of Structural Engineers

Artificial intelligence implementation checklist

Organisational readiness	Define an AI policy	Clearly outline your organisation's AI policy. Prepare policy statements for the three AI use scenarios: Internal use of AI tools. AI tools used directly by stakeholders. AI tools developed for external stakeholders. Ensure transparency and share your policy with all stakeholders. Review and update the AI policy regularly to reflect evolving risks, technologies, and regulations.	
	Appoint AI leadership	Identify an AI lead or point of contact within the organisation.	
		Define roles and responsibilities for AI implementation, particularly in larger organisations.	
	Set up reporting mechanisms	Establish clear processes for reporting AI-related concerns, including anonymous reporting options.	
		Document and track issues, ensuring prompt action on safety concerns.	
Risk management	Conduct risk assessments	Identify risks related to safety, security, sustainability, and legality.	
		Develop and maintain a risk and mitigation statement, updated at regular intervals (eg, quarterly or annually).	
	Safety mitigation measures	Ensure senior engineers review AI-generated designs.	
		Avoid using AI tools for high-security or sensitive projects unless properly secured.	
		Implement version control for datasets to mitigate risks of data poisoning.	
		Train junior engineers before granting access to AI tools to prevent deskilling	
	Sustainability measures	Assess the carbon footprint of AI-generated designs.	
		Use AI only when its benefits outweigh its environmental impact (eg, power usage for large datasets).	
		Consider the societal impact of reducing workforce roles due to AI adoption.	
	Legal compliance	Confirm compliance with local laws, such as GDPR and copyright laws.	
		Verify data ownership before using or storing client-provided datasets.	
		Ensure external AI tools do not unintentionally share proprietary data.	
Data governance software and hardware management	Develop data management policies	Define how data will be collected, stored, and disposed of.	
		Ensure consistent data collection methods across the organisation.	
		Implement high-quality standards for datasets, with oversight to prevent biases or inaccuracies.	
	Protect data security and privacy	Control access to datasets (eg, restrict access to specific teams or roles).	
		Prevent unauthorised use of sensitive structural data.	
		Use secure storage solutions (eg, on-premises or vetted cloud-based services).	
	Inventory software and hardware	Document all software and hardware used for AI applications.	
		Regularly update this list, including licenses and usage purposes.	
	Evaluate deployment methods	Determine whether AI software will run locally or remotely.	
		Decide on data storage locations (on-premises or cloud-based).	
	Monitor software performance:	Continuously assess software for compatibility with current standards (eg, updated design codes).	
		Plan for retiring outdated tools (eg, when standards like Eurocodes are updated).	
Workforce training and competence	Provide training on AI Tools	Offer training sessions on AI concepts and their application to structural engineering.	
		Ensure engineers understand AI limitations and implications for design safety.	
	Promote knowledge sharing	Encourage collaboration and information exchange within teams to build AI expertise.	
		Designate an internal AI resource hub for employees	
Lifecycle management	Plan AI tool lifecycles	Define a lifecycle for each AI tool, from implementation to retirement.	
		Periodically assess the suitability of tools for current projects and standards.	
		Document development and resource needs for each stage of the lifecycle.	
	Develop adaptable policies	Ensure policies are scalable to fit the organisation’s size and evolving needs.	
		Maintain flexibility to adapt to changes in AI technologies and regulations.	