

Using AI Responsibly at TEG

All TEG employees, contractors, officers, and directors (“**TEG Workers**”) are responsible for how they use Artificial Intelligence (“**AI**”) at TEG. This guide is designed to **empower boldness in clear boundaries** by encouraging responsible AI use that is aligned with our **AI Governance Policy**.

All TEG Workers must comply with this guide when using AI products at TEG. A failure to comply with this guide may constitute a breach of the TEG Code of Conduct and could result in disciplinary action.

If you have questions about this policy or using AI at TEG, please contact our IT Team or TEG Legal.

Top 7 Responsible AI Use Rules

- 1. Review all generative AI outputs for accuracy and reliability before use, publication or sending in an email.** Generative AI products may ‘hallucinate’ or produce outputs that are misleading, incomplete, inaccurate or out of date. Be careful using generative AI products to conduct research, generate material, or in processes that may have a financial impact.
- 2. Do not input personal information, customer data, financial data, source code or commercially sensitive information into a public AI product (such as Chat GPT, or Otter AI).** Instead, use Gemini, or other AI products approved by our IT Team. Unless an AI product has been approved by our IT Team, we don’t know how our data is being used, or who it is shared with.
- 3. Use AI as a support tool, not a substitute for judgement.** You should not rely solely on AI to make important decision, such as hiring, promotions, disciplinary actions, legal advice, financial approvals, or decisions relating to director’s duties. Be aware that AI products may reflect or amplify biases, and outputs should be checked for fairness and accuracy. You may use AI to assist, but important decisions should be made by a human, using your own professional judgment.
- 4. Do not use generative AI to create new brand assets or logos, or source code without approval.** We value and want to own the IP in our brand and the tech we build. New brand assets and source code created using generative AI may not be owned by TEG. Ask your manager if your use of AI for this purpose has been approved by TEG Legal, or contact TEG Legal if you are unsure.
- 5. Take accountability for your AI agents.** You are responsible for the acts of your AI agents. AI agents you create should only be used to perform tasks that are low-risk, repetitive, or administrative (e.g. scheduling meetings, generating reminders, or summarising documents). You should require your AI agent to seek your active confirmation for any irreversible or financially binding actions. Agentic AI should not be used to impersonate a human or make important decisions. More advanced AI agents should only be created in coordination with the AI enablement team and IT Team.
- 6. If you don’t know the capabilities and limitations of an AI product, find out.** If you are unsure about how to use an AI product, it is your responsibility to seek guidance from your manager or the IT Team.
- 7. Do not use your company card to purchase AI product licences or subscriptions.** We may already have a TEG subscription, or a similar product that you can use. You can make a request to get new AI products approved by contacting the [Enterprise Technology Service Desk](#). If you do make a purchase on your company card, you will be asked to reimburse TEG.

Prohibited AI Uses and Activities

The following uses of AI are strictly prohibited at TEG, as they may breach privacy or anti-discrimination laws, constitute unethical behaviour, and/or otherwise expose TEG to significant financial, reputational or legal risk.

- Inputting personal information or commercially sensitive information into an AI Product unless done so in a secure TEG environment approved by our IT Team.
- Unauthorised use of synthetic media (e.g. deepfakes, or voice cloning) to impersonate a TEG Worker, artist, fan or other individual.
- Unauthorised use of generative AI to produce material containing any brand logos or marks, or other material protected by copyright (e.g. to generate a Disney character).
- Using an AI Product to re-identify individuals from anonymised or de-identified datasets unless explicitly authorised under law and approved by TEG Legal.
- Using an AI Product to infer sensitive personal information (e.g. health status, sexual orientation, religious beliefs) about an individual.
- Using an AI Product to manipulate, mislead, or influence users in ways that circumvent valid consent or privacy choices (e.g. dark patterns, AI-generated nudge techniques to override opt-outs).
- Using someone's physical traits (e.g. their face, voice, or fingerprints) to analyse or make assumptions about them.
- Inferring emotions in a workplace (e.g. at a TEG office or a show) unless strictly for safety reasons.
- Evaluating an individual's likelihood of committing a workplace or criminal offence, based solely on personal characteristics (e.g. their age, race, gender, appearance, where they live, or past behaviour).
- Fully relying on an AI Product to perform a task or make a decision that a TEG Worker is expected to perform, without consultation with your manager.
- Using the output of an AI Product in client communications without validating information provided (e.g. relying on research conducted solely using Gemini in a client presentation or a sales pitch).
- Using customer, employee, or partner data to train AI models without appropriate de-identification, consent (where required), or contractual safeguards.
- Sharing personal information with third party AI vendors or platforms without conducting a privacy impact assessment and entering into appropriate data sharing agreements. For more information, contact [TEG Legal](#).
- Collecting, generating, processing, or storing personal information using an AI Product without a lawful basis or outside of an approved platform for personal information storage. For details on approved platforms, refer to the [Customer Data Storage, Handling and Disclosure Policy](#).
- Development of a facial recognition database by using untargeted scraping from the internet or CCTV footage.

Training

All TEG Workers are responsible for ensuring they attend or access the AI training that is offered to them – this may be general training, role specific training, or training to use a particular AI product.

You must make yourselves aware of the limitations of the AI products you are using, including understanding what data can be safely inputted into a particular AI product, and the degree to which outputs may be bias, misleading, incomplete or inaccurate. If you are unsure on how to responsibly use an AI Product, speak to your manager or contact the IT Team.

Reporting concerns

If you have any concerns, big or small, about how an AI product is operating, you should report it to:

- [Enterprise Technology Service Desk](#) for third party procured software; or
- **Ticketek IT Support on Jira** (i.e. Event IT, System Support, or Technical Operations) for internally developed software.

If you suspect a more serious AI Incident has occurred, you should report it immediately. An “AI Incident” is an event or series of events resulting from the use or operation of an AI product that causes:

- harm to individuals, groups or TEG (e.g. personal safety issues, privacy breaches, discrimination, reputational damage, or significant financial loss);
- a significant unintended deviation from an AI Products expected outputs or behaviour; or
- a breach in applicable law, regulation or TEG policy.

If you receive notification of an actual or suspected AI Incident from an external AI Product user (e.g. a venue client or fan), this must be immediately reported.

When reporting, provide as much detail as possible (what happened, when, which AI product, and any screenshots or outputs if available). All reports of AI Incidents will be taken seriously and reviewed. Reporting in good faith is encouraged – you will not face negative consequences for raising a genuine concern, even if it turns out to be a false alarm.

Document Information

Version Number	1.0
Last Update	04/09/2025
File Name	Responsible AI Use Guide
Responsible Executive (Role Position)	Global Chief Technology Officer and Group General Counsel / Company Secretary

Document Revision and Approval History

Version	Issue Date	Author	Comments	Approved By
1.0	05/09/2025	Olivia Henderson		Ben Groom and Amanda Luhrmann