AI Governance Policy

1. Purpose

This policy outlines TEG's approach to responsible development, procurement and use of artificial intelligence ("**AI**"). It is designed to **empower boldness in clear boundaries** by promoting AI driven innovation and operational efficiencies, while ensuring compliance with laws and alignment with TEG's risk appetite.

2. Scope

This policy applies to any AI Product developed, procured or used at TEG.

Definition of AI Product

An "**AI Product**" is an engineered or machine-based system that can, for a given set of objectives and with varying levels of autonomy, influence real or virtual environments by:

- generating outputs such as predictions, recommendations, or decisions; and/or
- performing tasks or sets of tasks, such as purchasing a ticket on behalf of a fan, booking meeting or reporting a cyber incident.

AI Products captured by this policy include:

- proprietary AI Products built in-house (e.g. Genome AI or operational insights dashboards);
- AI Products procured from a third party by TEG (e.g. Gemini);
- existing third party software procured by TEG that includes an AI feature (e.g. BrazeAI); and
- third party AI Products used by a TEG Worker without approval from the TEG IT Team (e.g. Chat-GPT).

Application to TEG Workers

All TEG employees, contractors, officers, and directors ("**TEG Workers**") who interact with an AI Product at TEG must comply with this policy. Misuse of AI products in breach of this policy may constitute a breach of the TEG Code of Conduct and could result in disciplinary action, up to and including termination of employment or engagement.

The below terms describe the responsibilities that different TEG Workers have with respect to AI Products.

- An "**AI User**" is a TEG Worker who uses an AI Product at TEG. This person is responsible for their own use of an AI Product in line with the Responsible Use of AI Products requirements (see section 4).

- The "**AI Product Owner**" is the person authorised to deploy the AI Product at TEG with the authority of the Global IT Director (for third party procured AI Products) or the Portfolio Product Manager (for AI Products developed in-house). This person is responsible for ensuring the AI Product is aligned with the TEG Responsible AI Principles (see section 3), an AI Risk Assessment in conducted (see section 5), a Tech & Data Legal Review is conducted if necessary (see section 6), AI Monitoring systems are in place as needed (see section 7), and the AI Product is appropriately documented (see section 8).

- The "**AI and Data Governance Council**" is responsible for AI governance and organisational level oversite.

3. TEG Responsible AI Principles

All AI Products deployed at TEG must align with the TEG Responsible AI Principles. **The AI Product Owner is responsible for ensuring that the AI Products they are responsible for align with the TEG Responsible AI Principles.**

Accountable	• Responsible individuals (i.e. AI Product Owners) should be identified and accountable each AI Product throughout its lifecycle. • AI decision making should not be fully automated (i.e. without human involvement) if the decision has a significant impact on an individual or group, such as hiring or promotions.
Fair	• The output of AI Products should not produce result that unfairly discriminate against individuals or groups. • AI Products should be inclusive and not be unfairly inaccessible to groups of individuals, such as people with disability. • Individuals should be able to challenge an AI Product's output if it has a significant impact on them or affects their legal rights, such as a refund request.
Transparent	• Individuals should be aware if they are engaging with an AI Product or if an AI Product is monitoring or evaluating them.
Reliable	• AI Products should reliably operate in accordance with its intended purpose on par with industry best practice.
Secure and privacy protected	• AI Product design, implementation and use should protect data security, including employing privacy by design principles and aligning with the relevant Privacy Policy.
Lawful	• AI Products and their use should not cause TEG or TEG Workers to contravene applicable laws, including privacy, anti-discrimination, employment and consumer laws.

4. Responsible use of AI Products

TEG Workers are responsible for how they use both AI Products and their outputs. All TEG Workers must comply with the **Using AI Responsibly at TEG** guide when using AI Products at TEG.

If you want to use a new AI Product at TEG, you may make request through the Enterprise Technology Service Desk.

TEG Workers are responsible for ensuring they attend AI Training (see section 10) and make themselves aware of the limitations of the AI Products they 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.

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.
- 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.
- 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 re-identify individuals from anonymised or de-identified datasets unless explicitly authorised under law and approved by TEG Legal.
- 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.
- 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).
- 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).
- Development of a facial recognition database by using untargeted scraping from the internet or CCTV footage.
- 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).

5. AI Risk Management

AI Risk Assessment

The deployment of AI Products may give rise to unique risks that should be considered during the scoping phase of the AI Product procurement or development. **The AI Product Owner is responsible for ensuring that an AI Risk Assessment in conducted using the AI Risk Matix below, and ensuring the 'Required Action' is undertaken** (see the right hand column of AI Risk Matrix).

For existing third party software procured by TEG that includes an AI feature, an AI Risk Assessment should be conducted when the procurement contract is renewed, or the software use is otherwise under consideration.

AI Risk Matix

Use the 'Guidance for Assessment' and 'Examples' columns to assist in determining an appropriate Risk Rating for the AI Product. If the assessment produces a borderline result, the higher Risk Rating should be adopted. If any of the Guidance for Assessment factors in the High Risk category are present, the AI Product is High Risk.

Risk Rating	Guidance for Assessment	Examples	Required Action
No or Minimal Risk: *May cause insignificant or minor financial, legal or reputational harm and is unlikely to occur.*	• Off the shelf product from an existing TEG vendor • Used to perform a narrow procedural task • Does not process or generate Personal Information* or commercially sensitive information • Does not involved automated decision making without human review • Internal TEG use only • TEG does not need to own the intellectual property rights in the output	• A spelling and grammar checker • A spam filter existing email software • An AI feature in exiting TEG software that makes design suggestions (provided that the software is not used to create brand assets such as logos) • Generating an Excel formular using a natural language query	• No action required under this policy.
Limited Risk: *May cause financial, legal or reputational harm that is more that insignificant or minor but is either unlikely to occur or impacts can be remediated.*	• Off the shelf product from new or existing vendor • May process limited Personal Information* or sensitive commercial information in a closed TEG environment • Does not involve automated decision making without human review • Internal TEG use only • TEG does not need to own the intellectual property rights in the output	• Using a data analytics tool to forecast event attendance or sales internally • A chat bot accessible only to TEG Workers for a narrow function, such as providing information about TEG policies • Scheduling assistant • One to one biometric authentication (e.g. facial recognition to unlock a laptop).	• Implement AI Monitoring in accordance with section 7, as required. • Document the AI Product in accordance with section 8. • If personal information is processed or generated contact Privacy & Data Counsel to determine if a Privacy Impact Assessment is required..
High Risk: *Financial, legal or reputational harm is a real possibility and may not be fully remediable; or may result in significant financial, legal or reputational harm even if unlikely to occur.*	• Bespoke or highly customised AI Product • Accessed or used by customers, clients, business partners or the public • Processes Personal Information* or sensitive commercial information outside of a closed TEG environment • Processes or generates Sensitive Information** or customer data • Automates or materially assists with a decision with significant impacts for an individual (e.g. employee performance decisions) • Automates or materially assists with a decision with legal impacts (e.g. customer refund decisions, or decisions relating to director's duties) • AI Products designed to influence the behaviour of individuals or groups • TEG wants to own the intellectual property rights in the output (e.g. source code or brand assets)	• A chat bot to respond to customer queries • AI Product used in hiring decisions or to place targeted job advertisements • Facial recognition used at venues to identify ticketholders • AI Product used by Event Partners to generate ticket pricing suggestions • AI Product used to generate or assist with drafting source code	• Initiate a Legal Tech & Data Review (**TDL Review**) in accordance with section 6. • Implement AI Monitoring in accordance with section 7, as required. • Document the AI Product in accordance with section 8. • If personal information is processed or generated contact Privacy & Data Counsel to determine if a Privacy Impact Assessment is required.
Unacceptable Risk	• See Prohibited AI Uses and Activities in section 4		• Not to be deployed or used at TEG

****Personal Information** means any information or an opinion about a reasonably identifiable person. ***Sensitive Information** means personal information about an individual's racial or ethnic origin, political opinions or associations, religious or philosophical beliefs, trade union membership or associations, sexual orientation or practices, criminal record, health or genetic information or biometric information.*

6. Tech & Data Legal Review

Any AI Product assessed as High Risk requires a Tech & Data Legal Review (**TDL Review**), which can be initiated by contacting TEG Legal. **The AI Product Owner is responsible for ensuring the TDL Review is initiated** during the scoping phase of the AI Product procurement or development or upon contract renewal.

A member of TEG Legal shall conduct the review in consultation with the AI Product Owner and present the final recommendations back to the AI Product Owner, which may include:

- no recommendations, meaning the AI Product is approved for deployment;
- recommendations for additional deployment safeguards, such as product disclaimers, product terms and conditions, changes to data flows, incident reporting functions, human involvement in automated decision making, and/or additional AI Monitoring (see section 7); or
- a recommendation that the AI Product use case exceeds TEG's acceptable risk tolerance and should not be deployed.

Any deviation from the recommendations must be approved by the Managing Director of the relevant business unit, in consultation with TEG Legal.

7. AI Monitoring

The AI Product Owner is responsible for monitoring and ensuring the AI Product's ongoing compliance with the Responsible AI Principles and its intended use and function. The type and extent of monitoring required will depend on the risk rating (with higher risk ratings requiring higher levels of monitoring), and tendency for the AI Product to 'drift' from its intended purpose or experiences changes in the quality or reliability of its output. An AI Product with a "No or Minimal Risk" rating will not require AI specific monitoring under this policy.

AI Monitoring may include but is not limited to:

- investigating and responding to alerts of defects and issues from TEG Workers, clients, or customers;
- testing the AI Product at regular intervals to identify and mitigate any bias or AI drift;
- requiring the AI Product supplier to provide periodic performance reports; and/or
- use of performance monitoring tools such as logging and visualisation, or automated anomaly detection and alert systems.

8. Documentation

All AI Products must be recorded in the relevant technology register.

- Proprietary AI Products built in-house should be recorded in the **Technology Component Catalogue**.
- AI Products procured from a third party by TEG should be recorded in the **Third Party Subservice Register**.

The additional information that needs to be recorded for AI Products includes: the AI Product's intended use, AI Product Owner, Risk Rating, AI Monitoring protocols (if relevant), and any AI Incidents (see section 9) (recorded promptly after the incident arises).

A copy of all LTD Reviews and recommendations must be retained by TEG Legal

9. AI Incident Reporting

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 a TEG Worker notices and suspects an AI Incident, or a near miss, they should report that 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 a TEG Worker received notification of an AI Incident from an external AI Product user (e.g. a venue client or fan), this must be immediately reported.

10. Training

All TEG Workers must complete training on the responsible use of AI Products at TEG, the TEG Responsible AI Principles, and their responsibilities under this policy. Additional roles based training may be required for AI Product Owners, the AI and Data Governance Council, specific business units, users of specific AI Products, the Senior Leadership Team, and Directors.

11. Policy review

This policy will be reviewed at least annually or when prompted by:

- a change in legislation or regulations affecting AI;
- a material change in technology; or
- a material AI-related incident or feedback from internal or external stakeholders.

Document Information

Version Number	1.0
Last Update	04/09/2025
File Name	AI Governance Policy
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