

AI USAGE POLICY

October 2026

[intertek.com](https://www.intertek.com)





1. Purpose

Intertek's AI Usage Policy establishes requirements for the responsible development, procurement, deployment, and use of artificial intelligence ("AI") systems within the Company. The objectives of this Policy are to:

- Promote innovation and productivity through AI.
- Protect confidential, personal, and proprietary information.
- Ensure compliance with applicable laws, regulations, and contractual obligations.
- Manage legal, ethical, operational, and reputational risks.
- Maintain appropriate human oversight of AI-generated outputs.

2. Scope

Intertek's AI Usage Policy applies to:

- All Intertek employees, contractors, temporary staff, and third parties.
- All forms of AI, including generative AI, machine learning models, automation tools, and embedded AI capabilities in enterprise software.
- Both company-provided and publicly available AI tools.
- Any organisational or customer data into, processed by, or generated through AI systems.

3. Guiding principles

The Company will only use AI in a manner that is:

Responsible

AI systems must be deployed and used in accordance with ethical, professional and legal standards, including the EU AI Act.

Transparent

Users must be trained under Intertek's AI Usage training and understand when AI is being used and must disclose material AI-generated content where appropriate. The company will fully disclose whenever AI agents are interacting with external parties.

Human-centered

AI assists human decision-making but does not replace accountability for business decisions. Critical decision-making will always involve human review and oversight, with the ability to intervene, override or escalate as necessary.

Secure

AI systems must protect confidential, proprietary, and personal information.

To ensure security, we have an established enterprise-wide risk management framework, which guides our approach to managing and mitigating cyber risk across our global operations. The framework underpins our enterprise security policies, standards and controls, which define how we govern, identify, protect, detect, respond and recover from potential threats. Elements of the framework include vulnerability analysis, internal auditing and testing, robust access controls, continuous system monitoring, structured incident response processes, and established resilience and recovery plans.

Fair and non-discriminatory

AI outputs and models must be regularly monitored for bias and unintended discriminatory impacts.



4. Permitted uses

Users may use approved AI tools for:

- Research and analysis.
- Drafting communications and reports.
- Summarising documents.
- Coding assistance.
- Productivity and workflow enhancement.
- Customer service support, subject to appropriate review.

All outputs must be reviewed by a qualified employee before external use or reliance.

5. Prohibited uses

Users may not:

- Input confidential, privileged, non-public, or customer information into unapproved AI tools.
- Use AI to make legally binding decisions without human review.
- Use AI to generate misleading, deceptive, discriminatory, or unlawful content.
- Upload source code, trade secrets, or regulated data without authorisation.
- Represent AI-generated output as verified fact without validation.
- Use non-approved AI tools.

6. Acceptable usage

Users must:

- Comply with all Intertek policies including Confidentiality, Information Security, Data Protection and Data Classification, and follow Intertek's guidelines on Access Control, and AI Governance.
- Only use Approved AI Tools or Intertek Owned or Developed AI Systems when AI functionality is required for business tasks.
- Ensure that any data entered into AI systems complies with Intertek data classifications, customer confidentiality requirements and any other contractual requirements.
- Validate AI generated outputs for accuracy, bias, appropriateness, and completeness
- Label as AI-generated content when applicable and when outputs are being shared with third parties.
- Maintain human oversight and apply professional judgement when acting on AI generated recommendations.
- Report incorrect, harmful, or suspicious AI behaviour to the Global Cyber Security Team.

7. Human oversight

Employees remain accountable for all work products generated using AI.

Prior to use in business activities, users must:

- Review AI outputs for accuracy.
- Verify factual statements and citations.
- Assess legal, reputational, and regulatory risks.
- Correct errors, hallucinations, or biased outputs.



At a Group level, our AI risk committee has overall responsibility for risk decisions and compliance. Any errors, harm or non-compliance relating to AI use will be investigated through our AI risk committee and Group Compliance function in accordance with the company's standard compliance review processes.

8. Intellectual property

Users must:

- Respect third-party intellectual property rights.
- Ensure AI-generated content does not infringe copyrights, trademarks, or proprietary rights.
- Consult Legal regarding significant external publication or commercialisation of AI-generated content.

9. Regulatory compliance

All AI activities must comply with:

- Data protection laws.
- Industry regulations.
- Consumer protection requirements.
- Contractual obligations.
- Company policies and codes of conduct.

10. Training

Employees using AI tools must complete required AI training covering:

- Responsible AI principles.
- Data protection.
- Cybersecurity.
- Prompting best practices.
- Risks associated with AI-generated content.

11. Review

Intertek's AI Usage Policy is reviewed annually and when significant changes occur in AI regulations, the technology landscape or to Intertek risk.

12. Violations

Failure to comply with Intertek's AI Usage Policy may result in disciplinary action, including termination of employment and other legal remedies where appropriate.

Authorised by the Group General Counsel and Head of Risk and Compliance, Intertek Group plc.

Name: Todd Andrews

Signed:

Date: 1 October 2026