The Content Division: AI Policy

The Content Division has developed an Artificial Intelligence (AI) policy which outlines how we use AI tools to assist in our service delivery, the tools we have approved to use internally, and the extreme importance of human oversight. Our team is responsible for the content they produce with assistance from AI programs.

Scope

This policy applies to all employees of The Content Division who use AI tools in their work. AI tools refers to assistants and programs such as ChatGPT, Midjourney, Dall-e, and AI tools in features in design, audio and video editing software such as the Adobe Suite.

Ethical Use and Compliance

1. Data Privacy: Always ensure that AI tools comply with data protection regulations (e.g., GDPR, CCPA). Do not input sensitive or personal client information into AI systems unless explicitly permitted.
2. Transparency: Inform clients when AI tools are used in their projects. Maintain transparency in all communications regarding AI-generated content.
    a. The Content Division's Terms of Engagement have been updated to reflect this.

Quality Control

1. Human Oversight: All AI-generated content must be reviewed by a human before delivery to clients. This ensures quality, accuracy, and alignment with the brand.
2. Accountability: Employees are responsible for the content they produce using AI tools.

Training and Skill Development

1. Continuous Learning: Participate in ongoing training sessions on AI tools and best practices.
2. Skill Enhancement: Develop skills that complement AI capabilities.

Operational Efficiency

1. Integration: Use AI tools that are integrated into The Content Division's workflows to maximise efficiency – eg. Adobe Suite.
2. Tool Selection: Use approved AI tools that meet the agency's standards for usability and effectiveness. See approved list at the end of this document.

Client Relations

1. Value Proposition: Communicate the benefits of AI to clients, including efficiency and enhanced creativity.
2. Customisation and Personalisation: Use AI to support personalised marketing efforts while maintaining a human touch.

Security and Risk Management

1. Cybersecurity: Ensure all AI tools are secure and updated regularly to protect against cyber threats.
2. Risk Assessment: Regularly assess the risks associated with AI use and develop contingency plans.

Do's and Don'ts

Do's

- Do use AI for repetitive tasks such as data analysis, report generation, and initial content drafts.
- Do ensure all AI-generated content is reviewed and edited by a human before client delivery.
- Do maintain transparency with clients about the use of AI in their projects.
- Do participate in training sessions to stay updated on AI tools and ethical use.

Don'ts

- Don't input sensitive or personal client information into AI systems without explicit permission.
- Don't rely solely on AI for final content delivery without human oversight.
- Don't use AI tools that have not been approved by The Content Division.
- Don't ignore ethical considerations such as bias and fairness in AI-generated content.

Examples of AI Use

Acceptable Use

- Content Drafting: Using AI to create initial drafts of articles, social media posts, or marketing copy, followed by internal editing.
- Data Analysis: Utilising AI for analysing large datasets to extract insights and trends.

Unacceptable Use

- Sensitive Data: Entering confidential client information into AI tools without permission.

- Final Approval: Delivering AI-generated content to clients without a thorough internal review.
- Unapproved Tools: Using AI tools that have not been vetted and approved by The Content Division for security and effectiveness.

By adhering to this policy, employees of The Content Division can leverage AI tools effectively and ethically, enhancing both their productivity and the quality of service provided to clients.

Approved tools

When selecting AI tools that comply with GDPR (General Data Protection Regulation), it is important to choose providers that prioritise data privacy and security. Here are some AI tools known for their compliance with these regulations:

AI Tools Compliant with GDPR

OpenAI (e.g., ChatGPT, DALL•E)

- Features: Natural language processing models capable of text generation, summarization, and conversation.
- Compliance: OpenAI aims to comply with GDPR through data minimisation, secure data handling, and providing users with control over their data.
- Use Cases: Content creation, customer service automation, and virtual assistants. Visual image development to create first drafts and concepts.

Google Cloud AI

- Features: AI and machine learning tools for natural language understanding, vision, translation, and AutoML.
- Compliance: Google Cloud AI provides tools and resources to help customers meet GDPR, such as data encryption, audit logs, and user consent management.
- Use Cases: Natural language processing, image recognition, and translation services.

Adobe Suite

- Features: Generative Fill in Adobe Photoshop, AI editing features in Adobe Audition, Premier Pro and After Effects.

- Compliance: Refer to Abode AI User Guidelines
- Use Cases: Image editing ie. remove objects, add in or change objects or to do a sky replacement etc. Video editing ie. make backplates for videos, adding in windows or paintings in walls etc in the background. Audio editing ie. clean up any audio, remove unwanted sounds or sharpen audio if it is a poor recording.

Midjourney

- Features: Creative and image generation.
- Compliance: Note Midjourney's Privacy Policy.
- Use Cases: Photograph generation and creative concept generation as a first draft and inspiration for development.