Guidelines for Use of Generative AI Tools

The purpose of these guidelines is to ensure that staff use approved AI tools in a manner that is consistent with our values and ethical guidelines, and in accordance with our data privacy controls and client commitments.

These guidelines set out the standards we require staff to observe when using approved AI tools or including them in any services or deliverables to clients. When using approved AI tools for any business use, you must comply with the following guidelines:

(a) **Confidential information and Data protection.** Approved AI tools have been vetted and contracted to secure our data and prohibit training third party AI models. You may input or upload Miroma or a clients' confidential information or personal data into approved AI tools (subject to any contractual restrictions or obligations). Please look at our data flow chart to ensure that you are using these compliantly. Usage should still adhere to the following principles:

- only use confidential information that is necessary for the purpose;
- only staff with appropriate authorisation should upload or process confidential or personal data in approved AI tools and access should be restricted to those who require it for their role;
- where Miroma has approved use of AI which includes the processing of personal or sensitive information, data protection compliance is paramount. This includes the requirement to comply with the principle of data minimisation (i.e. only using personal data that is limited to what is necessary for your purposes) and ensuring that you have a legal basis for processing any personal or special category data;
- where possible, anonymise or pseudonymise data before inputting into an approved AI tool to reduce privacy risks;
- avoid including direct identifiers (names, contact details, IDs) unless absolutely necessary and justified for the purpose;
- ensure deletion where retention is not required and adhere to your company's data retention policy;
- every new AI initiative or use case involving personal data should be subject to a data protection impact assessment (DPIA). If you have a new use case involving personal data please complete the form here.

Please see our Group Data Protection Policy for further information on what constitutes personal data and how to handle it.

(b) **Intellectual property rights and AI application terms.** Be aware of any intellectual property rights owned by third parties, such as copyright or trade mark rights when using generative AI, and if in doubt, speak to a member of the Legal team. For example:

Prompts

(i) do not enter anything into a prompt that is likely to result in the output infringing third party intellectual property rights (such as copyright or trade marks). Avoid prompts that ask an AI to create work 'in the style of' named artists, brands, or photographers.

(ii) keep records of all prompts used to create deliverables for clients. Doing so helps provide evidence if issues were to arise regarding, for example, IP infringement, misuse of confidential information or personal data.

Output

(i) review all output to try to ensure that no deliverables to be used by the company, either for its own purposes or for delivery to a client, contain any content that is likely to create a legal risk, for example, images of well-known people or third party rights, such as copyright works or trade marks (or substantial parts of them). When in doubt, ask a member of the Legal team.

(c) **Discriminatory or biased language.** Never input offensive, discriminatory or inappropriate content as a prompt into an approved AI tool or use offensive, discriminatory or inappropriate content which is generated as output by an approved AI tool. Avoid generating, or using, output which is biased, or which perpetuates stereotypes. You must always remember the principles set out in the Diversity, Equality and Inclusion policy when using any approved AI tool.

(d) **Be secure.** You must apply the same security measures we apply to all our IT applications when using generative AI and always comply with our IT Security and Acceptable Usage policies. This includes using strong passwords, updating applications as required and not installing software from external sources without authorisation from your IT provider. When adding an AI tools into an existing workflow (for instance, using a new AI plugin in a project management software), be cautious about any impact on data integrity, security or compliance. Ensure the AI integration does not inadvertently change how data is stored or shared.

All concerns, questions, suspected breaches or known breaches in relation to IT security must be referred immediately to your IT provider. If personal data is involved, please also refer this immediately to the Legal team.

(e) **Review outputs.** Generative AI has the potential to produce inaccurate outputs or hallucinations (outputs which may appear to be believable but are inaccurate or fabricated). There is also a risk that the output is biased, outdated, inappropriate or otherwise offensive. This means that critical thought must be applied to all outputs of approved AI tools; they must always be fact and sense checked before being relied upon for business purposes and reviewed and edited to ensure content is appropriate and for proper context and accuracy.

(f) **Guardrails**. Guardrails are the rules given to generative AI technology requiring it to avoid certain topics or answers. For example, due to regulatory concerns, this might include financial advice. This may also include avoiding topics or answers around potentially unlawful matters such as the creation of dangerous objects. The generative

AI may also be programmed to avoid subjects that it is not well-trained to answer. You should take this into account when assessing any outputs created using generative AI technologies.

(g) **Tone.** It is important that internal and external communications drafted using generative AI applications are carefully tone-checked to make sure that they are pitched appropriately and reflect the correct tone and degree of formality for their purpose and the intended recipient. Balance AI assistance with human review to preserve authenticity and context.

(h) **Ethical and responsible use**. Always use approved AI tools ethically, responsibly and in accordance with Miroma's and your company's values. You must not use generative AI in any way that could be considered discriminatory, or could amount to defamation, harassment, intimidation or bullying, or in any way that could harm the reputation of another. You must not use generative AI to create illegal content or for illegal purposes.

(i) **Monitoring.** Treat AI systems as needing ongoing supervision. Things to be careful of include model "drift" or performance degradation over time, new types of errors, or changes in the data that could affect outputs. If you notice an AI tool that used to be accurate is now making more mistakes, or an AI model is being used in a context different from what it was intended for, please raise this with the AI Team.

Other general usage rules

In addition to the guidelines above, you must:

- when using any of the approved AI tools for business purposes, use your work email address for log-in purposes.
- not in any way provide or suggest any endorsement or recommendation by Miroma of any third party generative AI tool.
- where you use generative AI, protect your login credentials and ensure that any generative AI accounts that you hold are not accessible to unauthorised third parties.
- comply with the terms and conditions of the generative AI technology that you use (unless such terms and conditions are in conflict with or contradict the Miroma or company policies or your terms of employment, in which case you should seek advice from the Legal team);
- when circulating, publishing or otherwise making available the output externally, clearly identify that the output has been created using, or with the assistance of, generative AI technologies.

Note: In all permitted uses, human oversight, review, and common sense are required. AI supports your work, but final decisions must remain human. All staff are ultimately still responsible for agency output. Double-check critical outputs and ensure they make sense. When used appropriately, AI should enhance your work without compromising ethics, quality, or compliance.

Prohibited uses

Certain uses of AI are strictly forbidden due to high risk or misalignment with our values. Do NOT use AI in the following ways:

Disclosing Sensitive or Confidential Information – Never input, upload, or expose Miroma or clients' confidential, proprietary, or personal data into any AI tool that is not explicitly approved for that purpose. This includes pasting confidential text into public generative AI tools (like the free version of ChatGPT). Treat any information given to an external AI as if you are publishing it publicly. Customer data, financial records, trade secrets, source code, or personal identifiers must not be provided to AI tools unless they have been vetted and contracted to secure our data.

Bypassing Data Protection or Security Controls – Do not use AI tools to try to work around security measures or to access data you are not authorised to see. For example, using an AI script to scrape restricted information, or employing AI to decrypt or hack systems, is strictly prohibited. AI must not be used for any illegal, fraudulent, or unauthorised purposes.

Automated Decision-Making Without Human Oversight – Do not deploy an AI tool to make decisions that have legal, financial, HR, safety, or similarly significant effects on individuals without human review and approval. For instance, fully automating job candidate screening processes using AI is not allowed. Such decisions require a human in the loop to prevent unfair or incorrect outcomes.

Generating Inappropriate or Misleading Content – Employees must not use AI to create content that causes or may cause significant risk or harm to individuals, groups or the reputation of Miroma, including hate speech, harassment, defamation, or explicit content. Likewise, do not use AI to deceive or mislead others by impersonating humans (e.g. deepfakes) or producing fake news, phishing emails, or fraudulent messages. Any AI-driven communication must be honest and not used to manipulate unethically.

Violating Intellectual Property (IP) Rights – Do not use AI to generate or disseminate content in ways that infringe on copyrights, trademarks, or licenses. For example, asking an AI to produce text or images by copying a proprietary source, or using code from an AI that is directly lifted from open-source repositories without proper attribution or license compliance, is forbidden. Always respect IP rights – when in doubt, consult Legal or avoid using that AI output.

Ignoring Regulatory or Compliance Requirements – Any AI use that would put Miroma in breach of laws or regulations is prohibited. Do not circumvent compliance processes by deploying unapproved AI solutions in sensitive areas.

Overriding professional advice - Advice that is typically given by licensed professionals, like accountants or lawyers, should only be obtained by the appropriate licensed professional and not AI. (This should not prevent AI being used to assist professionals in their work provided that the work is validated before sharing).

Any breach of the above prohibited uses is subject to disciplinary action and/or further investigation. Always err on the side of caution – if an AI use case feels questionable or risky, assume it is not allowed and seek guidance first.

Guidance for Tools Not on Approved List

This section provides practical expectations and tips for specific classes of AI tools that employees commonly use.

Generative AI Tools (e.g. ChatGPT, Bard, DALL·E, etc.)

- **Appropriate Uses**: Generative AI tools may be used for ideation, draft non-sensitive documents or summarise public information. For instance, ChatGPT can help you compose an initial email draft, and an image generator can visualise a concept for an internal presentation. Use these outputs as starting points that you will refine.

- **Data Input**: Do not input confidential or personal data into generative AI tools unless they are an approved AI tool. Public generative AIs may learn from your inputs or store them. If you must discuss something sensitive, abstract or anonymise the details. (E.g., instead of using a real client's name or data in a prompt, use a placeholder or similar scenario.) The same caution applies to uploading files – do not upload internal documents into an AI service that isn't an approved AI tool.

- **Fact-Checking and Accuracy**: Always fact-check any factual statements it provides. If ChatGPT writes a paragraph that includes statistics or claims, verify them from a reliable source. Do not assume the output is correct just because it looks confident. The employee using the tool is responsible for the accuracy of the final content.

- **Tone and Quality**: Review the tone of AI-generated text to ensure it fits the intended audience. Edit for clarity, conciseness, and appropriateness. Similarly, check AI-generated images for any odd or off-brand elements. Minor anomalies (like distorted text in an image, or subtle biases in how people are depicted) need correction or the output should be discarded.

- **Originality and IP**: While generative AI creates "new" content, it is trained on existing works. Be mindful of potential copyright issues. Use generative outputs as drafts and don't assume they are wholly original. For important assets, have the output reviewed for originality. When in doubt, involve the Legal team to ensure we're not infringing someone else's IP inadvertently.

- **Avoiding Abuse of Generative AI:** Do not use generative AI to create disallowed content (see Prohibited Uses). For example, don't generate fake customer reviews or any content meant to deceive.