

# AI Acceptable Use Policy Template

For Jamaican organizations. Prepared by Syxel Technologies Limited.

## How to use this template

This template gives you a complete starting point for an AI acceptable use policy. Delete this page before you adopt it.

- Replace everything in [square brackets] with your own details, and delete examples that do not apply.
- Decide who owns the policy and who advises on personal data (your Data Protection Officer, if you have one).
- Fill in the Approved AI Tools Register in Appendix A with the tools you allow and the settings staff must use.
- Check the information categories in section 6 against how your organization already classifies information.
- Review the policy with management, and with a legal adviser if you handle large amounts of personal or sensitive data.
- Train staff on the policy, give them the one-page quick guide in Appendix D, and collect signed acknowledgements (Appendix C).

This template is general guidance, not legal advice. It was prepared by Syxel Technologies Limited with the Jamaica Data Protection Act, 2020 in mind. For help adapting it, choosing approved tools or training your staff, contact [sales@syxeltech.com](mailto:sales@syxeltech.com) or (876) 218-8241.

# [Organization] Artificial Intelligence (AI) Acceptable Use Policy

|                |                                            |
|----------------|--------------------------------------------|
| Policy owner   | [Role, e.g. Operations Manager]            |
| Approved by    | [Name, role]                               |
| Version        | [1.0]                                      |
| Effective date | [Date]                                     |
| Next review    | [Date, 12 months after the effective date] |

## 1. Purpose

This policy explains how people working for [Organization] may use artificial intelligence (AI) tools. It lets us benefit from AI while protecting our customers, staff, information and reputation, and keeping us within the law, including the Data Protection Act, 2020 (the "Act").

## 2. Scope

This policy applies to:

- all employees, contractors, consultants, interns and volunteers who use AI tools for [Organization] work, on any device, including personal phones and computers;
- all AI tools, including chat assistants (for example ChatGPT, Microsoft Copilot or Google Gemini), writing, image, video and voice tools, meeting transcription and note-taking tools, coding assistants, and AI features built into software we already use, such as email, office, accounting and customer management systems.

## 3. Definitions

| Term          | Meaning                                                                                                                                                                        |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AI tool       | Any software that uses artificial intelligence to generate, summarize, analyze, translate or transcribe content, or to make predictions or recommendations.                    |
| Approved tool | An AI tool listed in the Approved AI Tools Register (Appendix A), used with the account type and settings listed there.                                                        |
| Personal data | Information about a living person who can be identified from it, directly or indirectly, such as a name, address, phone number, TRN, account number, photo or voice recording. |

| Term                     | Meaning                                                                                                                                                                                                                                                                                 |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sensitive personal data  | Personal data the Act protects more strictly, such as information about health, genetic or biometric data, racial or ethnic origin, political opinions, religious beliefs, trade union membership, sex life, and criminal offences or proceedings. See the Act for the full definition. |
| Confidential information | Information that is not public and could harm [Organization], our clients or partners if disclosed, such as contracts, pricing, financial records, plans and client files.                                                                                                              |
| AI output                | Anything an AI tool produces: text, images, audio, video, code, summaries, translations or recommendations.                                                                                                                                                                             |

## 4. Roles and responsibilities

| Role                                    | Responsibilities                                                                                                                                                                                     |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Policy owner: [role]                    | Keeps the Approved AI Tools Register up to date, reviews tool requests, arranges training and reviews this policy.                                                                                   |
| Data Protection Officer: [name or role] | Advises on any use of personal data with AI, decides whether a data protection impact assessment is needed, and handles possible data breaches, including reporting to the Information Commissioner. |
| Managers                                | Make sure their teams know and follow this policy, and approve how AI is used in their area.                                                                                                         |
| Everyone covered by this policy         | Follows this policy, completes training, checks AI output before using it, and reports problems straight away.                                                                                       |

## 5. Approved tools and accounts

- Only use AI tools listed in the Approved AI Tools Register (Appendix A), for the uses and information categories listed there.
- Use the work accounts [Organization] provides. Do not use personal accounts or free consumer versions for [Organization] work unless the register allows it.
- Keep the settings required in the register. Where a tool offers it, the setting that lets the provider use our inputs to train its models must be turned off.
- Do not install AI browser extensions, plug-ins, add-ins or apps that can read your email, documents, calendar or screen without approval.
- To request a new tool or a new use of an approved tool, complete the request form in Appendix B. [Role] will check its security, where it stores data, how the provider uses our information and

its contract terms before deciding.

## 6. What information you may enter

Before entering anything into an AI tool, decide which category it falls into. If you are unsure, treat it as the higher category or ask **[role]**.

| Category                | Examples                                                                                             | Approved tools                                                                               | Any other AI tool |
|-------------------------|------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|-------------------|
| Public                  | Published website content, press releases, public reports, marketing material                        | Yes                                                                                          | Yes               |
| Internal                | Internal procedures, routine meeting notes, drafts with no client or personal details                | Yes                                                                                          | No                |
| Confidential            | Contracts, pricing, financial records, client information, unpublished plans, source code            | Only if the register allows it                                                               | No                |
| Personal data           | Customer and employee records, names with contact details, TRNs, account numbers, CVs, photos        | Only if the tool is approved for personal data and the use complies with the Act (section 9) | No                |
| Sensitive personal data | Health and medical information, biometric data, criminal records, religious or political information | Only with written approval from the Data Protection Officer                                  | No                |
| Security information    | Passwords, PINs, access codes, API keys, network and system details                                  | Never                                                                                        | Never             |

Remove names and other identifying details whenever the task does not need them. For example, ask for help with "a customer complaint about a late delivery" rather than pasting in the customer's email.

## 7. Acceptable uses

Used within the rules above, AI tools can help you to:

- draft and edit emails, letters, reports, proposals and social media posts;
- summarize long documents, articles or meeting notes;
- brainstorm ideas, outlines and options;
- research a topic as a starting point, then confirm the facts from reliable sources;
- write or explain spreadsheet formulas, scripts and code, which you test before use;
- translate text or rewrite it in plainer language;
- prepare training material, frequently asked questions and templates;

- [add uses specific to your organization].

## 8. Prohibited uses

You must not use AI tools to:

- process information that section 6 does not allow for that tool;
- make, or effectively make, decisions about hiring, pay, promotion, discipline or dismissal, credit, insurance, pricing for individuals, or medical or legal matters, without a qualified person reviewing the information and making the decision;
- create content that is discriminatory, harassing, offensive, misleading or defamatory;
- impersonate a real person, including creating fake images, video or voice recordings of anyone ("deepfakes");
- give customers professional, legal, financial or medical advice that a qualified person has not reviewed;
- get around security controls, monitoring or other [Organization] policies;
- record, transcribe or summarize meetings or calls without telling the participants, and getting their agreement where required;
- upload material we do not have the right to use, such as copyrighted, licensed or another organization's confidential material.

## 9. Personal data and the Data Protection Act

When AI tools are used with personal data, the Act's data protection standards still apply. In particular:

- Use personal data only for a specific, lawful purpose that the people concerned would expect, and only the minimum needed for the task.
- Keep personal data accurate, keep it no longer than needed, and keep it secure, including within the AI tool and in any saved chats.
- Before using AI with personal data in a new way, ask the Data Protection Officer whether a data protection impact assessment is needed.
- Many AI providers process data outside Jamaica. Personal data may only be transferred overseas where the Act allows it, so the Data Protection Officer must confirm this before a tool is approved for personal data.
- People have rights under the Act, including to see the personal data we hold about them and to object to decisions about them that are made solely by automated means. Do not use AI to make decisions that significantly affect people without human review and the Data Protection Officer's approval.
- Where customer or staff data is processed with AI, make sure our privacy notices say so.

## 10. Checking AI output

- AI tools can be wrong, out of date or biased, and can invent facts, quotes, references, case law and statistics that look convincing. You are responsible for anything you produce or send with AI's help.
- Check facts, figures, names, dates, calculations and legal or regulatory references against reliable sources before using them.
- Have a second person review AI-assisted work that goes to [customers, regulators, the media or the board] before it is sent.
- Watch for bias or unfair assumptions, especially in content about people, and correct it.
- Test AI-generated code, formulas and automations before using them on live systems or data.

## 11. Being open about AI use

- Tell customers when they are dealing with an AI system, such as a chatbot, rather than a person, and give them an easy way to reach a person.
- Label AI-generated images, audio and video where people could mistake them for real.
- Disclose AI use where it is expected or required, for example in tenders, regulatory submissions or academic work that ask about it.
- Follow [Organization] guidance on labelling AI-generated content in our published material.

## 12. Intellectual property and confidentiality

- Check the provider's terms for who owns the output and how inputs are used. [Role] records this in the register.
- Before publishing AI output, check that it does not copy someone else's work, and do not ask AI tools to reproduce copyrighted material.
- Client contracts and non-disclosure agreements may forbid sharing client information with third parties, including AI providers. Check before using AI on client work.

## 13. Security

- Protect AI tool accounts with a strong, unique password and multi-factor authentication.
- Treat links, files and code that AI tools produce with the same caution as anything else from the internet.
- Be alert to AI-assisted scams, including cloned voices, fake video calls and convincing phishing emails. Confirm any unusual request for payment, passwords or information through a phone number you already know.
- Report a lost device or a suspected compromised account straight away.

## 14. Reporting problems

Report to [role, email and phone number] straight away if:

- you entered information into an AI tool that this policy does not allow;
- an AI tool shows you someone else's information, behaves unexpectedly or produces harmful content;
- you think someone is misusing AI tools.

Reporting quickly limits the harm, and you will not be penalized for reporting an honest mistake promptly. The Data Protection Officer will decide whether it is a personal data breach. The Act requires certain breaches to be reported to the Information Commissioner within 72 hours of becoming aware of them, so do not wait.

## 15. Training

- Everyone covered by this policy completes training on it before using AI tools for work, and a refresher every [12] months.
- Everyone signs the acknowledgement in Appendix C. [Role] keeps the signed copies.

## 16. Monitoring and breaches of this policy

- [Organization] may monitor how AI tools are used on its systems and accounts, in line with the law and our [IT acceptable use or monitoring policy].
- Breaking this policy may lead to loss of access to AI tools and to disciplinary action under our [disciplinary policy]. Serious breaches may also have legal consequences.

## 17. Review

[Role] reviews this policy every [12] months, or sooner if the law, guidance from the Information Commissioner, our tools or the way we use them change.

## 18. Related policies

[Delete any that do not apply.] Information Security Policy; Data Protection and Privacy Policy; IT Acceptable Use Policy; Records Retention Policy; Social Media Policy; Disciplinary Policy.

## Appendix A: Approved AI Tools Register

[Role] keeps this register up to date. Staff may only use the tools listed here, for the uses and highest information category shown.

| Tool        | Approved uses                   | Highest information category | Account and required settings                             | Approved by and date |
|-------------|---------------------------------|------------------------------|-----------------------------------------------------------|----------------------|
| [Tool name] | [e.g. drafting and summarizing] | [e.g. Internal]              | [e.g. work account only; training on our data turned off] | [Name, date]         |
|             |                                 |                              |                                                           |                      |
|             |                                 |                              |                                                           |                      |
|             |                                 |                              |                                                           |                      |

## Appendix B: New AI Tool Request Form

| Question                                                                           | Answer |
|------------------------------------------------------------------------------------|--------|
| Requested by and department                                                        |        |
| Tool name and website                                                              |        |
| What will you use it for?                                                          |        |
| Highest category of information you will enter (section 6)                         |        |
| Who else will use it?                                                              |        |
| Cost, and who pays                                                                 |        |
| For [role]: where is data stored, and is it used to train the provider's models?   |        |
| For the Data Protection Officer: personal data involved? Impact assessment needed? |        |
| Decision (approved, approved with conditions, declined) and conditions             |        |
| Decided by and date                                                                |        |

Appendix C: Staff Acknowledgement

I have read and understood the [Organization] Artificial Intelligence (AI) Acceptable Use Policy, version [1.0], and I agree to follow it. I understand that breaking it may lead to disciplinary action.

|                     |  |
|---------------------|--|
| Name                |  |
| Role and department |  |
| Signature           |  |
| Date                |  |

## Appendix D: Quick Guide for Staff

| Do                                         | Don't                                                  |
|--------------------------------------------|--------------------------------------------------------|
| Use approved tools with your work account  | Use personal or free accounts for work                 |
| Remove names and identifying details first | Paste in personal, client or confidential information  |
| Check facts, figures and references        | Send AI output without reading and checking it         |
| Have a person make decisions about people  | Let AI decide on hiring, discipline, credit or similar |
| Tell customers when they are talking to AI | Let customers think a chatbot is a person              |
| Report mistakes to [role] straight away    | Ever enter passwords, PINs or access codes             |
| Ask [role] if you are unsure               | Install AI extensions or apps without approval         |