Making Life Easier dynamics G-Ex

EAST COAST
Exploration House
37 Langton Road, Gympie
QLD 4570 Australia
+61 7 5482 6649

WEST COAST
48 Mulgul Road, Malaga
WA 6090 Australia
+61 8 9302 5700

www.dynamicsgex.com
sales@dynamicsgex.com.au
ABN 53 153 273 431

Generative AI Policy

About this policy

Dynamics G-Ex Pty Ltd have drafted this AI policy to establish clear guidelines and standards, ensuring that the Workforce understand and adhere to the accepted practices for using artificial intelligence within the workplace.

The use of generative artificial intelligence (generative AI) is transforming the way individuals are working. Informed and responsible use of generative AI has the potential to increase efficiency in the workplace, improve decision making and foster innovation. With these benefits come potential risks, including data protection breaches, copyright issues, the protection of confidential information, ethical considerations, and compliance with wider legal obligations.

We permit the informed and responsible use of authorised generative AI applications by the Workforce in carrying out identified business activities. The terms of this policy must be complied with when using generative AI to carry out business activities as it pertains to your role.

The purpose of this policy is to set out our rules on the use of generative AI in the workplace and how it should be adopted by the Workforce to ensure we maximise the benefits of generative AI while minimising any risks or concerns.

This policy is designed to be dynamic and responsive to the evolving landscape of generative AI and its implications for our workplace. We will continuously assess external circumstances and internal risk appetite, and this policy may be amended as necessary. Amendments will be made in alignment with the Employer's commitment to transparency and collaboration. This flexibility ensures that our approach remains relevant, proactive, and in the best interest of both the Employer and the Workforce, without forming part of any contract of employment or contract to provide services.

Who is responsible for this policy?

The board of directors (the Board) has overall responsibility for the effective operation of this policy. The Board has delegated responsibility for overseeing its implementation to the Marketing, IT and Operational Teams. Questions about the content of this policy or suggestions for change should be reported to your Direct leader, CCing Duane and Dan. To address evolving uses and understanding of generative AI, this policy is reviewed at least annually.

EAST COAST
Exploration House
37 Langton Road, Gympie
QLD 4570 Australia
+61 7 5482 6649

WEST COAST
48 Mulgul Road, Malaga
WA 6090 Australia
+61 8 9302 5700

www.dynamicsgex.com
sales@dynamicsgex.com.au
ABN 53 153 273 431

TERMINOLOGY USED IN THE POLICY

Terminology used in relation to generative AI can be confusing. We set out below some common terms used when describing AI and what they mean:

- Chatbot: A software application used to conduct an online chat conversation via text or text-to-speech.
- Generative AI: This refers to a type of artificial intelligence which can be used to generate new content (for example, text, code, images, videos, or music) (referred to as the output). The AI uses machine learning algorithms to analyse large data sets.
- Hallucination: Generative AI applications can produce outputs which may initially appear to be believable but are in fact fabricated by the system and often highly inaccurate. This is known as a hallucination.
- Large language models (LLMs): LLMs are a type of generative AI that can generate human like text in response to a prompt. They use deep learning techniques and massive data volumes to generate a response. LLMs are the underlying models that form the basis of generative AI applications.
- Machine Learning (ML): A subset of AI that enables systems to learn and improve from experience without being explicitly programmed.
- Natural Language Processing (NLP): The ability of a computer program to understand, interpret, and generate human language.
- Personal Data: Information related to an identifiable individual, including details that can directly or indirectly reveal their identity, such as names, identification numbers, location data, or online identifiers.
- Prompts: These are the inputs or queries that a user provides to the generative AI application to receive the required output. Prompts can be used by the generative AI application to further train the LLM.

SCOPE OF THE POLICY

This policy governs the use of generative AI technologies by the Workforce for all business-related activities. It encompasses the utilisation of generative AI tools both during official work hours and outside of work hours, irrespective of the device used (personal or company-owned) and the location of work (home, office, or remote settings). This policy is strictly applicable when the use of generative AI serves business objectives, ensuring comprehensive coverage and clarity on permissible practices within the professional context. Examples of generative AI enabling business to improve efficiency include:

Business Consulting

- Scenario Simulation: Utilize AI to simulate various business scenarios and predict potential outcomes.

- Proposal and Report Generation: Automate the creation of tailored business proposals and detailed reports.
- Custom Strategy Suggestions: Generate strategic recommendations informed by market trends and organizational data.

Marketing

- Content Creation: Generate marketing copy, social media posts, blog content, and campaign ideas efficiently.
- Visual Content Generation: Create graphics, videos, and images to enhance promotional campaigns.
- Email Marketing: Automate the generation of personalized email campaigns tailored to specific audience segments.
- SEO Optimization: Develop optimized content and keyword strategies to enhance search engine visibility.

Technology

- Code Generation: Streamline software development with AI-assisted code creation and debugging.
- Chatbots and Virtual Assistants: Enhance customer support and internal helpdesks using AI-powered conversational agents.
- Documentation Automation: Automate the creation of user guides, technical documentation, and FAQs.
- UI/UX Prototyping: Generate wireframes and design prototypes rapidly for development projects.

Recruitment

- Job Description Generation: Automate the drafting of customized job descriptions for diverse roles.
- Candidate Screening: Analyse resumes and rank candidates based on job-specific criteria.
- Interview Preparation: Generate role-specific interview questions and simulate interview scenarios.
- Offer Letter Drafting: Streamline the creation of professional offer letters and employment contracts.

Accounting

- Invoice Generation: Automate the creation of professional invoices and payment reminders.
- Financial Report Summarization: Summarize large datasets into concise and actionable financial insights.
- Expense Categorization: Automatically organize and categorize expenses for tracking and analysis.

- Tax Filing Assistance: Simplify tax calculations and compliance through AI-driven automation.

Marketing

- Content Creation: Generate marketing copy, social media posts, blog content, and campaign ideas efficiently.
- Visual Content Generation: Create graphics, videos, and images to enhance promotional campaigns.
- Email Marketing: Automate the generation of personalized email campaigns tailored to specific audience segments.
- SEO Optimization: Develop optimized content and keyword strategies to enhance search engine visibility.

Finance

- Portfolio Analysis: Generate insights into investment portfolios and suggest optimization strategies.
- Risk Assessment: Automate the assessment of financial risks based on historical data and trends.
- Budgeting and Forecasting: Use AI to create detailed financial forecasts and budget plans.
- Fraud Detection: Enhance fraud monitoring by identifying unusual patterns in financial transactions.

Travel

- Itinerary Planning: Generate customized travel itineraries based on user preferences and constraints.
- Cost Optimization: Analyse travel expenses and recommend cost-saving alternatives.
- Customer Support: Use AI-driven chat assistants to handle travel inquiries, bookings, and cancellations.
- Travel Document Generation: Automate the preparation of travel-related documents such as visas, itineraries, and confirmations.

AUTHORISED GENERATIVE AI APPLICATIONS

- All requests for new AI solutions or modifications to existing AI solutions are subject to the AI Access Review Process. This process entails completing an AI Assessment to evaluate risks, align operational expectations, and define desired business outcomes.

- We allow access to a wide range of publicly available generative AI applications and application add-ons for business purposes (referred to as authorised AI applications), which can be found in the Authorised AI Solutions List.

- The list of authorised AI applications may be updated at any time by Us. If you think there is any generative AI application that should be on the permitted list, please contact the IT Department.
- Use of authorised AI applications is subject to you ensuring the data protection options are set up. This will prevent the data entered being used by the LLM to train itself. If such options are unclear or are not available, please contact the IT Department for further clarification, before using it.
- To request access to AI solutions not currently in out AI solutions authorised list, please send an email to your direct leader, CCing Duane Menzies. The email must contain:
    - Requested AI tool and Link to their website
    - Reason for the request
    - Expected outcomes (What is the result expected)
    - What kind of data you are going to input in the requested AI tool.
    - Your level of confidence in operating it
    - Reason why it would not work within CoPilot Environment
    - Costs

PERMITTED USE

- Authorised AI applications must only be used by the Workforce for business purposes. Even if use is permitted, the fact that something is permissible does not mean it will necessarily be an appropriate business use of an authorised AI application.
- First before using any authorised AI applications for business purposes, you must first complete the mandatory training.

GUIDELINES FOR USE

When using authorised AI applications for business use, you must comply with the following guidelines:

- Employer data. Ensure that confidential, sensitive, or proprietary Employer, customer, supplier or employee-related data is not entered into the application as a prompt. This may include confidential, sensitive or proprietary data that has been deidentified or aggregated, as there is a risk that such data could be reidentified when combined with other data entered into a generative AI system or found elsewhere.
- Data protection. Ensure that any form of personal data is not entered into the application as a prompt.
- Intellectual property rights and licensing. Be aware of any intellectual property rights owned by third parties, such as copyright, database rights or trademark rights. Abide by any relevant licensing conditions regarding intellectual property rights in the authorised AI application's terms of use and ensure that third party proprietary data or material is not entered into the application as a prompt without the third party's permission. This includes ensuring, for example, that all or any substantial part of any copyright work owned by a third party is not inputted into the application as a prompt without the third party's consent.

- Discriminatory language. Never input offensive, discriminatory, or inappropriate content as a prompt.
- Be secure. You must apply the same security measures we apply to all our IT applications and always comply with our Cyber Security Policy. This includes using strong passwords, updating applications as required and not installing software from external sources without authorisation from the IT Department.

Review outputs. Generative AI has the potential to produce inaccurate outputs or hallucinations. There is also a risk that the output perpetuates biases, stereotypes, or inappropriate or otherwise offensive discriminatory practices. This means that critical thought must be applied to all outputs of authorised AI applications; they must always be fact and sense checked before being relied upon for business purposes and reviewed to ensure content is appropriate.

Decision making. Where a generative AI system is used to support a decision-making process, the outputs must be reviewed by you, and you must ensure that the output is accurate and appropriate in respect of the decision you have used the generative AI system to support.

Ethical and responsible use. Always use authorised AI applications ethically and responsibly. You must not generate content to impersonate, bully, or harass another person, or to search for or generate explicit or offensive content.

- Third-party add-ons. Be aware that third parties may build a service on top of generative AI applications. Avoid inputting any information or data into these add-ons. If in doubt about how add-ons may be operating in relation to an authorised AI application you are using, speak with the IT Department in the first instance.
- We recognise that some members of the Workforce may access generative AI applications via an application programming interface (API) rather than a web browser. Where appropriate, we may issue specific guidelines to Workforce members gaining access via APIs.

Monitoring and Data Loss Prevention (DLP)

We reserve the right to monitor all content (including but not limited to any prompts, or outputs) on any generative AI application used for business purposes. This will only be carried out to the extent permitted by law, for us to comply with a legal obligation or for our legitimate business purposes, including, without limitation, to:

- prevent misuse of the content and protect our confidential information (and the confidential and personal information of our customers, clients, and suppliers);
- ensure compliance with our rules, standards of conduct and policies in force from time to time (including this policy);
- monitor performance at work;
- ensure that our Workforce does not use our facilities or systems for any unlawful purposes or activities that may damage our business or reputation; and

- comply with legislation for the protection of intellectual property rights and to support proprietary rights in the output.

To achieve this, We will implement monitoring measures to identify and respond to potential Data Loss Prevention (DLP) violations.

Content Monitoring:

- We will monitor text, images, video, and other digital content shared with AI platforms for potential DLP violations.
- The monitoring will focus on identifying sensitive, confidential, or prohibited information to prevent it from being transmitted inappropriately.

DLP Alerts:

- If a potential DLP violation is detected, an alert will be triggered immediately.
- First Alert: The user will receive a notification, informing them of the detected violation and advising corrective action.
- Escalation Alert: The alert will be sent to the IT Operations (IT OPS) team for review and further investigation.

Data Handling:

- We will not intentionally collect or store any content beyond the specific content that triggered the DLP alert.
- All monitoring activities will be conducted in alignment with Our Data Protection and Cyber Security policies, ensuring minimal impact on user privacy.

Use of Data Loss Prevention Agent:

- We will utilise a DLP agent to monitor data flows between Our systems and external platforms, including generative AI tools.
- The agent will track the hash of the data as it moves, rather than storing or analysing the content itself.

Purpose and Scope:

- The primary purpose of implementing DLP is to prevent unintentional disclosure of sensitive or confidential information and to protect Our intellectual property.
- Monitoring will be limited to activities involving Our systems and approved AI platforms, focusing only on business-related activities.

Accountability and Oversight:

- The IT OPS team will oversee the monitoring and handling of DLP violations, ensuring timely and appropriate responses.
- Users will be educated on the importance of secure data handling and provided with resources to minimise risks when using AI platforms.

Record keeping

If using the outputs of authorised AI applications either directly or with minor alterations, you must clearly cite this in the work produced, for example as a footnote, by providing the web address and any sources used as prompts.

We will endeavour to implement an audit system to monitor and document all prompts and output received from authorised AI applications.

Training and technical support

To ensure comprehensive understanding and responsible use of authorised AI applications, We mandate annual awareness training accessible through the Learning Management System (LMS):

- 2024 KnowBe4 Security Awareness Training.
- AI Chatbots: Understanding Their Use, Risks, and Limitations in the Workplace.

Failure to complete the annual mandatory training may be treated by Us as a breach of this policy.

Costs

Employees are responsible for managing the appropriate use of authorised AI tools to avoid unnecessary expenses. The organisation will not reimburse costs arising from:

- Personal Subscriptions or Unauthorised Tools: Subscriptions to AI tools for personal use or the use of unauthorized third-party AI services.
- Excessive or Mismanaged Usage: Costs incurred due to excessive API calls, overuse of features, or repeated content generation requests that unnecessarily increase expenses.
- Credits or Additional Purchases: Purchasing extra credits or add-ons for AI tools without prior approval from the organization.
- Employees must ensure AI tools are used efficiently and only for business-related purposes. If unsure about potential costs, seek clarification before using the tool.

Breach of this policy

Breach of this policy may, where appropriate, result in disciplinary action up to and including dismissal or termination of your employment or engagement with Us. Where disciplinary action is appropriate, it may be taken whether the breach is committed during or outside normal hours of work and whether or not use of generative AI is on an individual's own device or one of Our devices, and whether at home, in the office or from a remote working location.

Examples of breaches include:

- Use of Unauthorised Applications: Employing unapproved AI tools that result in a data breach, compromising sensitive or confidential information.
- Sharing Sensitive Information: Entering proprietary, personal, or confidential data into AI platforms without ensuring compliance with Our data protection standards (as specified in the Data Protection Policy and Acceptable Use Policy).
- Perpetuating Biases or Stereotypes: Using AI-generated outputs that perpetuate harmful biases or stereotypes, leading to reputational damage, public backlash, or potential legal action against Us.
- Misinformation or Misuse: Disseminating inaccurate or inappropriate AI-generated content that harms Our credibility or relationships.
- Exceeding Authorised Use: Generating content or making requests outside approved business purposes, resulting in unnecessary costs or ethical breaches.

You are required to fully cooperate with any investigation into a suspected breach of this policy. This includes providing the organisation with access to any generative AI application you have used (whether authorised or unauthorised) and sharing relevant passwords and login details as necessary for the investigation.

Investigation Process

- Initial Assessment: Upon identifying or reporting a potential breach, the organisation will conduct an initial assessment to determine the scope and impact of the issue.
- Information Collection: Employees involved will be required to provide relevant information, including access to AI applications, logs, and related accounts, to facilitate a thorough review.
- Review and Analysis: The organisation will analyse collected data to determine whether a breach occurred and assess its impact on security, confidentiality, or reputational integrity.
- Resolution and Outcome: Based on findings, appropriate corrective actions will be taken, which may include addressing security gaps, disciplinary measures, or additional training for employees.

Cooperation in this process is essential to ensure a fair and efficient investigation while protecting the organisation's interests and compliance obligations. You must report any suspected or confirmed breach of this policy—whether it involves your own actions or those of another member of the workforce—immediately to your line manager and the IT Department. Prompt reporting ensures that We can take swift action to mitigate risks and address the issue effectively.

Steps to Report a Breach

Identify the Breach:

- Clearly document what occurred, including when and how the breach happened.
- Note any relevant details, such as the AI tool involved, the data or content affected, and the potential impact.

Notify Your Line Manager:

- Inform your line manager as soon as you become aware of the breach.
- Provide an initial overview of the incident and any steps you have taken to contain it, if applicable.

Contact the IT Department:

- Report the breach to the IT Department immediately, providing specific details about the incident.
- Share any documentation or evidence related to the breach, such as screenshots, logs, or communication records

Follow Guidance:

- Comply with instructions from your line manager or the IT Department, which may include additional reporting, containment actions, or providing further information for investigation.
- Do not attempt to address the breach independently unless instructed to do so.

Maintain Confidentiality:

- Do not share details of the breach with anyone outside of the reporting process to prevent escalation of risks or reputational damage.

Regulatory Compliance and Alignment

We are committed to aligning with and complying with current and emerging regulations governing the use of AI in the regions where We operate. This includes adherence to applicable laws, frameworks, and principles to ensure Our use of AI technologies is responsible, ethical, and transparent. Key regulatory frameworks and principles include, but are not limited to:

- European Union:
  a) EU Artificial Intelligence Act (AI Act): Ensuring compliance with requirements for trustworthy AI, including risk management, transparency, and accountability.
  b) General Data Protection Regulation (GDPR): Safeguarding personal data, ensuring lawful processing, and upholding data subject rights.
- United States:
  a) NIST AI Risk Management Framework: Adopting best practices for AI risk identification, mitigation, and governance.
  b) California Consumer Privacy Act/California Privacy Rights Act (CCPA/CPRA): Protecting consumer privacy and managing data responsibly.
- United Kingdom:

a) UK AI Strategy and Regulatory Approach: Following UK-specific guidelines for ethical and responsible AI use.

b) OECD Principles on AI: Promoting the use of AI systems that are inclusive, transparent, robust, and accountable, ensuring respect for human rights and democratic values.

- New Zealand:
  a) Privacy Act 2020: Upholding privacy protections, ensuring data collection, use, and storage comply with New Zealand's privacy regulations.
- Australia:
  a) Privacy Act 1988: Ensuring compliance with the Australian Privacy Principles (APPs) regarding the collection, use, storage, and disclosure of personal information, including when using AI tools.

AUTHORISED AI TOOLS – DEC/25

- Copilot (in the browser + across all MS Applications)
- ChatGPT (upon Request)

DEFINITIONS

Term	Definition
Workforce	This refers to all employees, officers, consultants, contractors, volunteers, interns, casual workers, and agency workers
Policy	This refers to the policy covered within this document known as the Global Generative AI Policy.
Visitor	Any person not an employee and its related group entities including customers and suppliers who may visit premises intermittently, usually for one day.