RHONDDA CYNON TAF COUNTY BOROUGH COUNCIL

ARTIFICIAL INTELLIGENCE
ACCEPTABLE USE POLICY

Version: FINAL V1.0 14.08.2025

Document Information	
Version:	1.0
Status:	Final Approved
Date Approved:	14.08.2025

CONTENTS

APPENDIX

1. INTRODUCTION

Rhondda Cynon Taf County Borough Council recognises Artificial Intelligence (AI) as a valuable asset that, when used appropriately, can significantly enhance the way we work. AI has the potential to improve productivity, support decision-making, and contribute to the Council's objectives.

It is important to understand that AI is a tool and that all employees must ensure content is appropriate, relevant, accurate and the employee remains responsible for their actions and the output.

This policy outlines the principles, responsibilities, and safeguards for the ethical and effective use of AI. It reflects a shared responsibility across the Council, from technical teams to managers and end users, to ensure AI is used safely, securely, and in line with Council values.

The Council is currently piloting the use of Microsoft 365 Copilot as its approved AI tool. At this time, Copilot is the only AI software authorised for use within the Council. The policy will be regularly reviewed and updated based on pilot feedback, evolving capabilities, and changes in legal, ethical, and operational standards.

2. PURPOSE

The purpose of this policy is to set out the Council's guidance on the acceptable use of AI in the workplace. This policy outlines how AI should be adopted to ensure maximum benefit whilst minimising any associated risks or concerns. The primary objectives are:

- **Efficiency and Productivity:** Encourage the use of AI, to improve business processes, and boost productivity across Council services.

- **Enhanced Work Experience:** Improve the overall employee experience by integrating AI into daily workflows, enabling staff to draft, summarise, and respond.

- **Accessibility and Inclusion:** Promote a more inclusive workplace by using AI to support individuals with diverse needs, including but not limited to neurodivergent people, disabled people, and anyone who may benefit from assistance with reading, writing, organising information, or reducing cognitive load.

- **Risk Management:** Identify and mitigate the potential risks associated with AI use, such as inaccurate outputs, misuse, or over-reliance on automated content.

- **Data Privacy and Security:** Protect personal and sensitive information by setting clear rules for data handling and ensuring that AI systems operate within secure and compliant environments.

- **Compliance with Laws and Regulations:** Ensure that the use of AI technologies adheres to all relevant legal requirements, such as data protection legislation and sector-specific regulations.
- **Ethical Standards:** Promote the ethical use of AI by establishing guidelines to prevent bias, discrimination, and other unethical practices in AI-generated content.
- **Transparency and Accountability:** Enhance transparency in AI processes and ensure accountability for decisions and actions influenced by AI tools.
- **Continuous Improvement:** Provide a framework for ongoing monitoring, evaluation, and refinement of AI systems to ensure they remain effective, reliable, and aligned with Council values.

3. DEFINITIONS & TERMINOLOGY

Key definitions and terminology relating to this policy can be found in Appendix I.

4. SCOPE

This policy applies to:

a) All employees of Rhondda Cynon Taf County Borough Council
b) Agency staff who access Council data and systems
c) Students (e.g. Social Work placements) who access Council data and systems
d) Elected Members & Co-opted Members when conducting official Council business (e.g. attending a committee)
e) External organisations receiving ICT services from the Council to conduct their business.

The policy applies regardless of working location (e.g. office, home or hybrid) and regardless of the device used.

This policy does not apply to schools, as they operate on separate platforms and are encouraged to use Hwb, the national digital platform.

5. LINKS TO OTHER POLICIES

This policy should be read in conjunction with the Council's overarching Information Security Policy and Data Protection Policy that can be found on RCT Source.

It should also be read alongside the following policies that support and integrate with the Council's currently approved AI tool, Microsoft 365 Copilot.

- M365 Teams Acceptable Use Policy
- Meeting Recording, Transcript & Copilot Protocol
- Internet & Email Acceptable Use Policy

Elected & Co-opted Members should refer to:

- Elected Members ICT, Internet & Email Acceptable Use Policy
- Co-opted Members ICT Agreement Policy

6. RISKS OF USING AI

While AI offers many benefits, it also presents risks that must be understood, managed, and addressed ethically. These risks fall into four main categories:

a) AI Outputs Risks

AI-generated outputs are not always reliable and may include:

- **Incorrect or Made-Up Information:** AI may generate false, misleading, or fabricated content that appears plausible.
- **Missing Key Details:** Important information may be omitted, leading to incomplete or unbalanced outputs.
- **Bias and Discrimination:** AI can reflect and reinforce biases present in training data, potentially leading to unfair or discriminatory outcomes.
- **Offensive Content:** Inappropriate or offensive language may be generated, especially if the AI was trained on biased or unfiltered data.
- **Complex Language and Nuance:** AI may struggle with context, tone, or subtle meanings in human language, leading to misinterpretation.
- **Ambiguous Queries:** Vague or unclear prompts can result in irrelevant or confusing responses.
- **Changing Information:** AI may not reflect the most current facts or developments, especially if it relies on static or outdated data.
- **Model Limitations:** AI systems can make errors or produce content that sounds confident but is factually incorrect.
- **Human-Like Responses:** AI is designed to sound fluent and authoritative, even when its output is inaccurate.
- **Language Settings:** Some AI tools may default to non-UK language conventions (e.g. American English).

These risks highlight the importance of human oversight. All AI-generated content must be reviewed carefully before use or distribution. Users must remain alert to these limitations and apply critical judgment when interpreting AI outputs. Further guidance on reviewing and managing AI outputs is provided in Section 7.4: Reviewing AI Outputs.

b) Ethical Risks

Ethical considerations are essential to ensure AI is used responsibly and for the benefit of all. These include:

- **Bias and Discrimination:** AI can reflect and reinforce unfair patterns in the data it learns from, leading to biased or unequal outcomes.
- **Unfair Outcomes:** AI may unintentionally disadvantage certain individuals or groups.

- **Risk of Harm:** Poorly designed or misused AI can cause harm to individuals or society.
- **Loss of Public Trust:** If AI is used in ways that are seen as unfair, unclear, or unsafe, it can reduce public trust in the Council and the services it provides.
- **Lack of Transparency:** It is not always clear how AI systems make decisions, which can make it difficult to explain or challenge their outputs.
- **Accountability Issues:** It can be unclear who is responsible for decisions made or influenced by AI.

c) Data Privacy & Security

- **Privacy Concerns:** AI may use or expose personal, sensitive, or commercially confidential information in ways that are not appropriate or expected. Data entered into some AI tools could be shared or made public, potentially breaching data protection laws, contracts, or intellectual property rights.
- **Security Breaches:** Information security risks and breaches may not be immediately obvious when using AI, especially when it is unclear what information is being used, where it is stored, or how it is being used.
- **Data Usage:** Information input into AI software may be accessed and used by the system provider to support the development and training of the AI model across the platform.

d) Legal & Compliance

- **Legal Uncertainty:** There remains legal uncertainty and complexity regarding how existing legislation applies to AI applications. An AI model can be acquired by another organisation or external operator, who may use legitimately collected information for unlawful purposes.
- **Unauthorised Applications:** A third party may build a service or software solution on top of an unauthorised AI application.

7. CONDITIONS OF AI USE

This section sets out the **key conditions of use** for AI tools. These conditions are designed to protect personal and confidential information, maintain the integrity of our work environment, and safeguard the wellbeing of users. **All users must follow these conditions of use.**

1) Approved AI Software:

Any use of AI must be **approved by** ICT & Digital Services. The approval process ensures that any AI tool meets the Council’s standards for data protection, privacy, and information security.

Copilot is currently the only AI software approved for use within the Council. **No other** AI tools or software are permitted for use within the Council, including free tools, browser extensions, or paid subscriptions. This exclusion applies to all publicly available AI platforms such as ChatGPT, Google Gemini, and any similar tools, which have not undergone the Council's security assessment or approval process. These tools are considered unregulated and pose potential risks to data privacy, security, and compliance. As such, their use is **strictly prohibited** for any Council-related activity.

2) **Prohibited Uses:**

Users are prohibited from:

- Using Council AI software for **personal purposes.**
- Using **personal AI software** for **Council business activities**.
- Using AI tools on a **personal device** for work-related purposes.

3) **Embedding AI into Working Practices:**

Heads of Service have a responsibility for embedding AI into working practices to ensure it is used safely, ethically, and in a way that supports service delivery and aligns with Council policy. This includes assessing risks, defining permitted use cases, implementing appropriate controls, supporting staff training, and maintaining oversight of AI use within their service areas. A separate AI Implementation Guidance for Heads of Service and Managers has been developed to provide detailed steps, and tools to support this process. All managers must refer to and follow this guidance when planning or overseeing the use of AI.

4) **Reviewing AI Outputs**

AI tools are powerful but not perfect. They generate responses based on patterns in data rather than human understanding, which means outputs can sometimes be inaccurate, misleading, or inappropriate. These risks are outlined in more detail in Section 6a and must be considered when using AI in any context.

Heads of Service and Managers are responsible for ensuring that AI outputs are reviewed consistently and appropriately within their service areas. This includes defining and communicating clear criteria for evaluating outputs such as accuracy, tone, and relevance. They must embed review procedures into service-level policies, training, and supervision. They should monitor outputs regularly, establish escalation routes for concerns, and encourage staff to report issues and contribute to continuous improvement.

All AI Users must treat AI outputs as drafts or suggestions rather than final answers. They are personally responsible for verifying the accuracy, relevance, and appropriateness of any AI-generated content before using it. Users must follow any service-specific review procedures or standards, report inaccuracies or concerns through the appropriate channels, and take full accountability for any content they use or share, regardless of whether it was generated by AI.

Failure to properly review AI outputs can lead to misinformation, reputational damage, or breaches of policy. Staff are accountable for the content they use or share, regardless of whether it was generated by AI.

5) AI Awareness, Training and Communication

Training is a mandatory requirement for all staff using AI tools. To ensure AI is used safely, ethically, and effectively, all users must complete the required training before access is granted. Heads of Service and managers are responsible for ensuring that training is delivered, understood, and embedded into local working practices.

Managers must ensure that all staff:

- Attend and complete mandatory system-level training provided by ICT & Digital Services, which covers the operation, features, and associated risks of the AI tool
- Receive service-specific training aligned with approved use cases and risk assessments, including practical guidance on local procedures, standards, and review processes
- Are fully informed of the capabilities and limitations of the AI tool
- Understand and follow all relevant Council policies
- Know how to report concerns or errors and where to seek support
- Have training embedded into onboarding, supervision, and ongoing development processes

All users of approved AI software **must**:

- Attend and complete all mandatory training before using AI tools
- Engage fully with both system-level and service-specific training
- Maintain up-to-date knowledge of how to use AI tools safely, ethically, and in line with Council and service-level policies
- Identify and communicate any training or development needs to their Line Manager
- Seek clarification or further support where needed to ensure confident and compliant use

6) Handling Personal and confidential Information in AI Tools

Users must not input or share personal or confidential data with AI tools (e.g. within a prompt) unless necessary for a legitimate Council purpose.

7) Unauthorised Information Access

AI tools generate outputs based on the information users have access to. If a user sees information in an AI-generated response that they believe they should not have access to, such as confidential, personal, or sensitive data they must take action to address it.

How this is resolved will depend on the type of data and where it is stored. The user should:

- Speak to their Line Manager to review whether their service access permissions are appropriate
- Raise a call with the ICT Service Desk if technical support is needed to adjust access
- Contact the owner of the relevant resource (e.g. a Teams channel, SharePoint site, or document) if the issue relates to shared content

These steps help ensure that access to information remains appropriate and secure, and that any incorrect permissions are corrected promptly.

8) Understanding AI Search Parameters and Constraints

Users must understand that AI tools can only generate responses based on the information they are able to access. This means that the quality and relevance of AI outputs will depend on where the tool is pulling data from and what the user has permission to access.

It is important that users are aware of these limitations when using AI tools, especially when interpreting results or relying on outputs for decision-making. Prompts and expectations should be shaped with these constraints in mind.

9) Submitting Feedback to AI Tools

Users are **not permitted** to submit feedback directly to AI tools as this may result in Council data being shared externally.

8. MONITORING, AUDIT & ENFORCEMENT

The use of AI is a valuable business tool; however, misuse can negatively impact the Council. As with any other Council system, such as email, internet, and other digital tools AI usage is subject to appropriate monitoring, auditing, and enforcement to ensure proper use and to protect the organisation, its data, and its users.

- **Council Property:** All Council-issued equipment, systems, software, tools, and any data held on them are the property of the Council, except where services are provided under a Service Level Agreement, in which case data ownership may rest with the partner organisation and will be governed by the terms of the SLA.

- **Monitoring and Review:** The Council reserves the right to access, monitor, and review a user's use of Council computer equipment, systems, facilities, and data covered by this policy (and related policies) without additional consent from the user. This includes bypassing any security settings (e.g., passwords) subject to authorisation by the Director of Human Resources and the Service Director, ICT & Digital Services.

- **Recording and Access:** All ICT activity (e.g., AI user activity, internet browser history, email traffic) is recorded. Access to and review of such equipment, systems, facilities, activity, and data will be undertaken strictly to the extent permitted or required by law, and as necessary and justifiable for legitimate Council business purposes, audit, and security, or where there is reason to believe that a breach of security or policy has occurred.

- **Restrictions:** The Council reserves the right to place restrictions on the use of AI tools and facilities at any time.

9. BREACH OF POLICY

Any breach of this policy or related policies may result in investigation and could lead to disciplinary action in line with the Council's procedures. Serious breaches may be referred to the Police or other external authorities.

The Council will cooperate fully with any investigation. If AI tools are used to generate or access offensive, discriminatory, or unlawful content, this may be treated as gross misconduct and could result in dismissal.

Anyone who believes this policy has been breached must report the matter to their Line Manager or Head of Service and the ICT Service Desk. Reports should follow the Council's procedure for reporting Information Security Incidents & Events.

Managers who become aware of a potential breach must consult with Human Resources and may instruct ICT Services or Internal Audit to investigate further.

All users are encouraged to report any actual or potential security incidents without fear of recrimination. Lessons learned from such events will be used to strengthen future controls.

Appendix I

Definitions & Terminology

Artificial Intelligence Software/Tool (AI Software, AI Tool)

- Is any application (app), software, or system that can independently adapt its own analytical methods and utilises artificial intelligence (including Generative and Agentic/ Algorithmic AI), machine learning, or other advanced algorithms to perform tasks, analyse data, or assist in making decisions. AI Tools may use Generative AI, Algorithmic AI, or both.

Generative AI (GenAI)

- Is a technology that can create new content in response to prompts, including but not limited to text, speech, and images (e.g., Microsoft Copilot).

Agentic AI (formerly referred to as Algorithmic AI)

- Is a technology that analyses data using machine-learning algorithms and can make decisions or predictions based on that data. These systems are increasingly capable of acting autonomously to complete tasks or achieve goals with minimal human intervention (e.g. Grammarly, Google Cloud AI Platform, Azure Machine Learning Studio).

Copilot

- Microsoft 365 Copilot is the Council's approved AI toolset, integrated into Microsoft applications to assist users with drafting, summarising, analysing, and automating tasks. It operates within the Council's secure Microsoft 365 environment.

AI Output

- The results or responses generated by AI tools, which can include text, images, predictions, decisions, or other forms of content. AI Output is produced based on the data and algorithms used by the AI tool, and it can vary in accuracy, relevance, and quality depending on the specific AI technology and its implementation.

Use Case

- A specific, approved scenario or task in which AI tools are applied to support or enhance a business process. Use cases define how AI is intended to be used within a service area, including the purpose, expected outcomes, and any associated controls or review procedures.

Document Control

Policy	ICT & Digital Services
Title	Artificial Intelligence Acceptable Use Policy
Author	Data Protection Officer, ICT & Digital Services
Owner	Service Director, ICT & Digital Services
Initial Policy Launch Date	14.08.2025
Review date	This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years.

Policy Approvals

This document requires the following approvals:

- Policy creation and major revisions: Information Management Board
- Minor revisions: Director of ICT & Digital Services (or delegated officer)

Version Control

Version No	Date Approved	Valid From Date	Valid To Date	Changes Made
1.0	Final approval 14.08.2025	14.08.2025		Initial policy approval