Use of Generative Artificial Intelligence Policy

POLICY:	**USE OF GENERATIVE ARTIFICIAL INTELLIGENCE**
Owner:	CIO
Author:	Greg Dwyer
Service Area:	ICT
Date:	October 2025
Review Date:	May 2026

Contents

1.0 Purpose

The purpose of this policy document is to provide a framework for the use of Generative Artificial Intelligence Large Language Models (GenAI) such as ChatGPT, Bard, Bing or other similar tools by council employees, contractors, developers, vendors, temporary staff, consultants or other third parties, hereinafter referred to as ‘users’.

This policy is designed to ensure that the use of GenAI is ethical, complies with all applicable laws, regulations, and council policies, and complements the council’s existing information and security policies.

The pace of development and application of GenAI is such that this policy will be in a constant state of development to ensure it continues to meet the needs of the council.

2.0 Scope

This policy applies to all users with access to GenAI, whether through council-owned devices or BYOD (bring your own device) in pursuit of council activities.

Use of GenAI must be in a manner that promotes fairness and avoids bias to prevent discrimination and promote equal treatment and be in such a way as to contribute positively to the council’s goals and values.

Users will only use GenAI for work-related purposes subject to written approval, and adherence to this policy. This includes tasks such as generating text or content for reports, emails, presentations, images, and customer service communications.

Particular attention must be given to governance, vendor practices, copyright, accuracy, confidentiality, disclosure, and integration with other tools.

3.0 Policy

3.1 Governance

Users are prohibited from accessing or using GenAI tools for council activities without prior written approval from the Chief Information Officer (CIO) of their intention to use, the reason for use, and the expected information to be input as well as the generated output and distribution of content. All departments to register AI systems in use, including generative models, with details on purpose, data sources, and risk level with the Information Governance Team. This supports transparency and accountability. Overall governance will be monitored and managed via the Corporate Information Governance Group (CIGG).

3.2 Vendors

Any use of GenAI technology in pursuit of council activities must be done with full acknowledgement of the policies, practices, terms and conditions of developers/vendors.

3.3 Copyright

Users must adhere to copyright laws when utilising GenAI. It is prohibited to use GenAI to generate content that infringes upon the intellectual property rights of others, including but not limited to copyrighted material. **All programmes must be pre-approved, if a user is unsure whether a particular use of GenAI constitutes copyright infringement, they must contact the legal team or Chief Information Officer before using GenAI.**

3.4 Confidentiality

It is strictly prohibited to enter confidential and personal information into a GenAI tool, as information may enter the public domain. Users must follow all applicable data privacy laws and organisational policies when using GenAI. **All programmes must be pre-approved, if a user has any doubt about the confidentiality of information, they must not use GenAI and contact the Chief Information Officer.**

3.5 Ethical Use

Users must not use GenAI to generate or disseminate content that is discriminatory, offensive, or in violation of council policies or applicable laws. **All programmes must be pre-approved, if there are any doubts about the appropriateness of using GenAI in a particular situation, users must consult with the HR team, Legal team, or the Chief Information Officer.**

3.6 Disclosure

Content produced via GenAI must be identified and disclosed as containing GenAI-generated information.

Example: This document contains content generated by Artificial Intelligence (AI). AI generated content has been reviewed by the author for accuracy and edited/revised where necessary. The author takes responsibility for this content.

3.7 Integration with other tools

Application programming Interface (API) and plugin tools enable access to GenAI and extended functionality for other services to improve automation and productivity outputs. Users must follow OpenAI’s Safety Best Practices:

- Adversarial testing
- Human in the loop (HITL)
- Prompt engineering
- “Know your customer” (KYC)
- Constrain user input and limit output tokens
- Allow users to report issues
- Understand and communicate limitations
- End-user IDs.

API and plugin tools must be rigorously tested for:

- Moderation – to ensure the model properly handles hate, discriminatory, threatening, etc. inputs appropriately.

- Factual responses – provide a ground of truth for the API and review responses accordingly.

4.0 Risk

Use of GenAI carries inherent risks. A comprehensive risk and Data Protection Impact assessments must be completed for any project or process where the use of GenAI is proposed. The risk assessment must consider potential impacts including legal compliance; bias and discrimination; security (including technical protections and security certifications); and data sovereignty and protection.

4.1 Legal Compliance

Data entered into GenAI may enter the public domain. This can release non-public information and breach regulatory requirements, customer or vendor contracts, or compromise intellectual property. Any release of private/personal information without the authorisation of the information asset owner could result in a breach of relevant data protection laws. Use of GenAI to compile content may also infringe on regulations for the protection of intellectual property rights. **Users must ensure that their use of any GenAI complies with all applicable laws and regulations and with council policies.**

4.2 Bias and Discrimination

GenAI may make use of and generate biased, discriminatory, or offensive content. Users *must* use GenAI responsibly and ethically, in compliance with council policies and applicable laws and regulations.

4.3 Security

GenAI may store sensitive data and information, which could be at risk of being breached or hacked. The council *must* assess technical protections and security certification of GenAI before use. **All programmes must be pre-approved, if a user has any doubt about the security of information input into GenAI, they *must* consult with the HR team, Legal team, or the Chief Information Officer.**

4.4 Data Sovereignty and Protection

While a GenAI platform may be hosted internationally, under data sovereignty rules information created or collected in the originating country will remain under jurisdiction of that country's laws. The reverse also applies. If information is sourced from GenAI hosted overseas, the laws of the source country regarding its use and access may apply. GenAI service providers must be assessed for data sovereignty practice by any organisation wishing to use their GenAI. **All programmes must be pre-approved, if a user has any doubts, they *must* consult with the Legal team, or the Chief Information Officer.**

Users *must* ensure that any GenAI tools being used are hosted in the UK or EEA countries.

5.0 Responsibilities

The Chief Information Officer has overall accountability and authority for the policy.

All Assistant Directors are responsible for the implementation of this policy in each of their respective service areas.

All users have the responsibility to adhere to this policy.

6.0 Related Policies, Standards and Guidelines

This policy *must* be read in conjunction with the:

- BYOD Policy
- Computer Usage Policy
- Data and Information Policy
- Data Protection Impact Assessment Policy
- Data Protection Policy
- Encryption Policy
- Information Classification Policy
- Information Security Policy
- Legal Responsibilities Policy
- Personal Data Subject Access Policy
- Risk Management Strategy
- System Access Policy
- Third Party Access Control Policy
- Third Part Data Sharing Protocol
- User Access Policy

All users *must* complete council-approved training on ethical, legal, and technical aspects of GenAI before being granted access to any GenAI tools.

7.0 Enforcement

The use of Generative Artificial Intelligence (GenAI) tools will be monitored and audited by the council, and users should have no expectation of privacy when using these systems. Any suspected breaches of this policy will be subject to investigation. All investigations will be reviewed on a case-by-case basis, taking into account the specific circumstances and context of each incident. Any user found deliberately contravening this policy or caught jeopardising or abusing the security of information *will* be dealt with under the Council’s Disciplinary Procedure. If a criminal offence is considered to have been committed further action *will* be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it apply to you, seek advice from your line manager, the HR team, Legal team, or the Chief Information Officer.

8.0 Review

This document *will* be reviewed on a bi-annual basis as a minimum or wherever there *are* changes of influencing circumstances due to the speed in which GenAI is changing.

Policy review *will* be undertaken by the Chief Information Officer, and will require reporting through CIGG before GMT and Overview Working Group sign off.

9.0 Acknowledgment

By using GenAI, users acknowledge that they have read and understood these guidelines, including the risks associated with the use of GenAI.

10.0 Document Attributes

Document Information

Title	Use of Generative Artificial Intelligence
Identifier	Use of Generative Artificial Intelligence
File Location	https://intranet.broxtowe.gov.uk/document-central/policies-procedures/information-management-policies/
Description	Details the policy, users responsibilities when using generative artificial intelligence
Keywords	GenAI; Generative Artificial Intelligence; Risks; Policy; Responsibilities
Format	MS Word
Author	Greg Dwyer
Owner	Chief Information Officer
Classification	OFFICIAL
Date Created	07 October 2025
Last Review Date	06 November 2025
Next Review Date	May 2026
Date to Dispose	12 months after later version produced

Document History

Date	Summary of Changes	Version
10/09/2025	Draft	0.1
07/10/2025	Final release	1.0
04/11/2025	Amended policy to be explicit as requested by the Overview Working Group	1.1
06/11/2025	Amended to change May to Will, bi-annual reviews, and approval through Overview Working Group.	1.2
17/11/2025	Amended Enforcement	1.3

Document Approval

Date	Name & Job Title of Approver(s)	Version
07/10/2025	Greg Dwyer – Assistant Director of Corporate Services	1.3

Distribution

Name / Group	Title
GMT	
Assistant Directors	
Heads of Service	

Coverage

Group
All users in the Council

End of Document