



(AI) Artificial Intelligence Policy

OWNER: AI GOVERNANCE BOARD

DATE: 18th September 2026

Document Control

Organisation	Cardiff Council
Title	Artificial Intelligence Policy
Owner	Artificial Intelligence Governance Board
Subject	Artificial Intelligence (AI)
Protective Marking	NOT PROTECTIVELY MARKED

Revision History

Revision Date	Revision	Previous Version	Description of Revision

Contents

Cardiff Council's Artificial Intelligence Policy (AI).....	5
Scope	5
Purpose	6
Considerations	6
Risk of using AI	7
Information Governance and Data Protection	7
Transparency	8
Equality Implications.....	8
Information and IT Governance Framework.....	9
Data Bias and Data Quality	10
Design Bias in Algorithms.....	11
Automated Decision Making	11
AI Technology	12
Chatbots	12
ChatGPT or other Large Language Models (LLMs) including Copilot.....	13
Procurement	15
Standards	16
Language Services	16
Roles and Responsibilities	17
Caldicott Principles	20

Executive Summary

Artificial Intelligence (AI) refers to computer systems engineered to execute tasks that traditionally require human cognitive abilities. The scope of AI continues to evolve as technological advancements become increasingly integrated into various aspects of daily life.

Notable examples of AI technology include:

- **Algorithms and predictive analytics** – *The system predicts which housing applications are most likely to need extra checks.*
- **Chatbots and virtual assistants** – *A chatbot answers residents' questions about council opening hours.*
- **Machine learning (ML)** – *The fraud system learns from past cases to spot suspicious claims.*
- **Remote monitoring solutions** – *Sensor's alert staff when a vulnerable resident hasn't moved for hours.*
- **Advanced smart technologies** – *Smart streetlights dim automatically when no one is nearby.*
- **Text editing and autocorrection tools** – *The email tool corrects spelling mistakes as you type.*
- **Automated language translation** – *A website instantly translates information into another language.*
- **Facial detection and recognition systems** – *Cameras automatically blur faces in public CCTV footage.*

Cardiff Council is committed to leveraging Artificial Intelligence (AI) responsibly to improve service quality, accessibility, and efficiency for all service users, members and employees.

AI offers transformative opportunities, from enhancing decision-making and automating routine tasks to improving digital engagement and service delivery. However, its use must align with ethical standards, legal requirements, and the Council's core values.

Council employees play a pivotal role in ensuring AI is implemented and used effectively. Staff are accountable for championing ethical AI practices that comply with GDPR, Welsh Language Standards, accessibility standards, and principles of transparency and fairness. This includes integrating AI in ways that meet organisational and community needs while preventing bias and unintended consequences.

Managers are responsible for building capability and confidence across teams by ensuring their teams are appropriately trained, fostering digital literacy, and promoting continuous improvement. Through strong governance and leadership, managers help embed AI in ways that strengthen trust, accountability, and deliver better outcomes for service users.

Service areas must ensure that all AI projects and related activities address necessary considerations, including risk assessment, accessibility compliance, and alignment with this policy and other applicable Cardiff Council policies. By doing so, they safeguard the integrity of the council, the deployment of AI and maintain public confidence.

Cardiff Council's Artificial Intelligence Policy (AI)

This policy applies to anyone who interacts with AI on behalf of the Council:

- All Cardiff Council Employees
- Members of Cardiff Council
- Suppliers and Contractors of Cardiff Council
- Temporary and Agency Staff engaging with Cardiff Council
- Volunteers for Cardiff Council
- All others using the Council's information or Systems.

Scope

This Policy is designed to complement current Council policies. All officers using Artificial Intelligence (AI) technologies are required to adhere to existing Council procedures and compliance obligations related to Information Governance, Data Protection, ICT, Welsh Language Standards, Cyber Security and Equality Diversity and Inclusion (EDI), including Single Impact Assessments, as outlined below.

This Policy outlines the Council's approach to AI and details the roles and responsibilities required for compliance with information standards and legislation.

All staff who use or plan to use AI are required to become familiar with this Policy and are responsible for ensuring transparency in its application. This applies to AI technologies that are being designed, developed, or procured by Cardiff Council, as well as the use of AI tools such as Large Language Models (LLMs) including, but not limited to, ChatGPT, Google Gemini and Microsoft 365 Copilot. It does not apply to existing AI technologies available through the Council's Microsoft licence, such as predictive text features in Microsoft Teams, Outlook, or Word.

Wherever possible, officers are expected to make use of the AI tools available within the Microsoft 365 suite of products (such as M365 Copilot) as the primary route before considering alternative options.

If the implementation of AI may affect employees or necessitate changes in working practices, please consult with HR People Services for guidance.

Purpose

AI is progressively being integrated into the public sector due to its significant potential to enhance the delivery of services.

When used responsibly and effectively, AI has the potential to enhance data management and utilisation, enabling the Council to operate more efficiently and provide more effective support to service users, council staff and suppliers.

In response to the development of innovative AI technologies, as well as related concerns regarding equality and data protection, this Policy establishes a comprehensive framework for the deployment of AI solutions within Council services.

Considerations

For some technologies it is clear that they use AI, but for others this is not always apparent. The following factors must be considered:

- *Does this facilitate decision-making, or is it responsible for making decisions?*
- *Does it support the delivery of information?*
- *Does it autonomously identify patterns in large volumes of data?*
- *Does it utilise Machine Learning, for example, learning to answer questions or solve problems?*
- *Does it predict or manage risks?*
- *Does it contribute to the allocation of resources or prioritisation of actions/ investigations/ inspections?*
- *Does it remotely monitor the well-being of individuals?*
- *Does it translate language?*
- *Does it analyse and/or act on data from its environment?*
- *Does it perceive and react to the world, for example, recognising visual information (e.g. objects, individuals) or speech?*
- *Does it store past data and predictions to inform future predictions?*
- *Does it remember, adapt or encourage changes to behaviour patterns?*

Risk of using AI

The risks inherent in the deployment of artificial intelligence continue to evolve. Key risk areas identified include:

- *Information Governance and Data Protection*
- *Transparency*
- *Equalities and Welsh Language Standards*
- *Data Bias and Data Quality*
- *Design Bias in Algorithms*
- *Automated Decision Making*

Information Governance and Data Protection

Where an AI system is using or collecting personal data, it will fall within the scope of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). This could include where Personal Data is being used to train or test AI, and/ or in the deployment of the technology.

The UK GDPR grants individuals rights where their Personal Data is being processed (used or created), particularly for automated decision making. These rights must be considered in the development and use of all relevant AI technologies.

Depending on the specific project or task, a Data Protection Impact Assessment (DPIA) may be required. In the first instance, a DPIA screening will be a useful tool with which to risk assess the proposed use of data. Done at an early stage, this can help officers mitigate many of the potential risks associated in the processing of Personal Data, especially regarding the proposed use of innovative AI technology. For more information on DPIAs and where it is mandatory to complete them, refer to the Council's Data Protection Policy.

[Data Protection Policy](#) In addition to the use of Personal Data, Officers intending to use AI technologies also need to consider the risks associated with the use of commercially sensitive data. If commercially sensitive data, or information that would not otherwise be released under Freedom of Information (FOI) requests is inputted into a Large Language Model (LLM) or processed in another AI technology, it may have then been inadvertently released into the public domain. Releasing such information provided to the Council in confidence could lead to legal proceedings. As such, it is vital that Officers appropriately consider the information they are using within AI projects or activities. For more information on Freedom of Information legislation, refer to the Information Governance Framework Policy.

All Officers proposing to use Personal Data (as defined in the Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR), and/ or commercially sensitive data in an AI project or activity must complete a DPIA and Single Impact Assessment and follow relevant processes about ICT Compliance and Risk.

In addition, all projects must follow the Council's Information Governance and Information Sharing policies and procedures.

[Information Governance](#)

[Information Sharing](#)

Transparency

In line with Information Governance and Data Protection protocols, the Council is required to uphold transparency throughout all stages of AI implementation. This entails clearly defining the intended purpose of the technology from the outset, assigning specific responsibilities and accountabilities to designated officers, and ensuring both operational staff and senior managers possess a comprehensive understanding of the AI system's functionality. Additionally, it is essential that service users are duly informed about the deployment and use of AI technologies and how it affects the user.

For AI initiatives that involve substantial public engagement or may significantly affect individuals, it may be required to complete the Algorithmic Transparency Recording Standard. Developed by central government, this standard is intended to help public sector organisations clearly communicate information regarding the algorithmic tools they employ, as well as the rationale behind their usage.

[Algorithmic Transparency Recording Standard - guidance for public sector bodies - GOV.UK](#)

Contact ICT Service Desk for more information & support: [ICT Service Desk Self Service Portal](#)

Equality Implications

Cardiff Council must follow the Public Sector Equality Duty under the Equality Act 2010. When working with AI technologies, the Council must assess and document their impact on protected groups—such as age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion and belief, sex, and sexual orientation—as well as care experience and socio-economic status. This is done through a Single Impact Assessment.

See the guidance for more details:

[Single Impact Assessment](#)

AI technologies can amplify existing biases, affecting protected groups like race, sex, and socio-economic background, and may lead to legal challenges. It is essential for the Council to carefully consider these risks when developing AI. AI may exhibit social or cultural bias, generate sensitive or inaccurate content, and produce plausible but erroneous outputs. **All content should be fact-checked before use.**

Digital exclusion is less relevant where AI is limited to internal use but must be addressed for customer-facing technologies. The Single Impact Assessment should consider digital exclusion and ensure alternatives are available for those unable to access AI benefits.

Information and IT Governance Framework

This policy should be read in conjunction with the following related policies, procedures and guidance.

- [Data Protection Policy and Procedure](#)
- [IT Security Policy](#)
- [Welsh Language Standards - The City of Cardiff Council](#)

Staff should familiarise themselves with the related policies, procedures and guidance set out within the Information and IT Governance Framework.

- Disciplinary Policy and Procedure
- Employee Code of Conduct
- Records Management Policy
- Payment Card Industry (PCI) Policy
- Remote IT Working Policy
- Mobile Devices Acceptable Usage Policy
- Removable Media Policy
- CCTV Policy and Code of Practice
- Body Worn Camera Council Wide Policy
- Social media & Online Participation Policy
- Data Protection Impact Assessment (DPIA) Procedure
- Legitimate Interests Guidance
- Freedom of Information and Environmental Information Procedure
- Requests for disclosure of information under the Data Protection Act 2018 Schedule 2 (usually Police requests)
- Schedule 2 Guidance
- Electronic Information Sharing Guidance
- Secure Destruction of Media Devices Policy
- Retention of Senior Management Mailboxes Procedure
- Data Protection Incidents Policy
- Asset Loss Procedure
- Protect Email Guidance
- Using Mobile Devices Abroad
- Clear Desk Policy & Securing Business Documents
- Code of guidance - mobile phones and driving
- iPad Guidance for Officers & Members
- Individual Rights (GDPR) Guidance
- Information Governance Strategy
- Monitoring Employees at Work Policy (DRAFT)

Data Bias and Data Quality

The integration of AI can result in the replication or amplification of existing inequalities through its outputs. Therefore, it is necessary to evaluate the data sources used for training and analysis to identify potential unconscious bias or discriminatory outcomes at the outset of an AI project.

When working with data, officers must check for and avoid “proxy variables.” These are pieces of information that seem important but do not directly relate to what is being measured. Using them can lead to unfair results. If proxy variables are found, they must be removed or corrected to keep the process fair and compliant.

In selecting data sources for AI training or processing, officers must assess data quality and suitability, including accuracy, completeness, relevance, and representativeness. This assessment supports compliance with the UK GDPR principles of data minimisation and accuracy and helps ensure that AI outputs are transparent, fair, and justifiable.

When choosing data sources for AI training or processing the ICO recommends:

- *Are there any gaps in protected characteristic information?*
- *Is the data sufficient for trend identification?*
- *Are any groups of people overrepresented or underrepresented in the data?*
- *Is protected characteristic information self-reported?*
- *Who owns the data?*
- *Does the data reflect the group of people, the intended audience or users?*
- *If the data quality is poor, Officers must improve data collection procedures before proceeding to develop an AI solution.*
- *Finally, do data sources include personal data or commercially sensitive information?*

Design Bias in Algorithms

In addition to data bias, the outputs of AI are influenced by human choices involved in its design:

- *the selection of data used to train it,*
- *the assumptions that inform the algorithm,*
- *and the way in which its outputs are interpreted and applied has the potential perpetuate existing bias or inequalities.*

Staff are advised to evaluate AI outputs carefully, recognising that bias may not always be apparent and that proxy data can sometimes indicate its presence.

Selecting suitable data that accurately represents service user demographics can help address these issues, but it is also necessary to address any assumptions within the algorithm. This process will include:

- *Using a Single Impact Assessment to conduct a robust assessment of existing processes or current practice that is proposed to be supported or replaced by AI before commencing the AI development.*
- *Where relevant, utilise the principles of inclusive design to involve people who will be affected by the technology, to ensure that the AI's assumptions or outputs to consider their experience.*
- *Devise a methodology to monitor the actual impacts and validate the AI's outputs, consider how assumptions may impact on the AI's outputs and thereby reflect the expectations of the those designing it.*

Automated Decision Making

AI systems do not always produce perfect or accurate outputs. They can generate false positives or negatives, which may reinforce bias or inequality. This risk increases when algorithms support or replace human decision-making, as incorrect or biased outputs may be applied without challenge. Where AI makes automated decisions that have legal or significant effects, additional obligations apply under Article 22 of the UK GDPR.

Human oversight and the ability to challenge AI outputs must always be maintained. This helps identify errors, prevent discriminatory outcomes, and highlight bias that can improve the algorithm over time. To do this effectively, Officers must understand how the algorithm works and receive any necessary training to identify issues.

Before using AI-assisted decision-making, Officers must carefully consider whether it is appropriate for their project or service and explore alternatives. If they choose to proceed, they must ensure:

- Compliance with all Article 22 UK GDPR requirements.
- A risk assessment of automated decision-making is completed.
- A responsible Officer is appointed and clearly identified for accountability.
- Processes exist to integrate AI into current workflows and flag incorrect or biased outputs.
- A scrutiny or audit process for AI outputs is in place.
- All necessary mitigations are applied.
- Decisions and assisted decisions are made in a non-discriminatory way.

Further guidance is available from the UK Government's Ethics, Transparency and Accountability Framework for Automated Decision-Making.

[Automated decision-making and profiling | ICO](#)

AI Technology

Officers should be informed about certain AI technologies classified as high-risk, such as chatbots, ChatGPT, and other Large Language Models (LLMs), including Copilot.

Chatbots

Chatbots are computer programs designed to simulate and process human conversation by responding to questions from users. More advanced chatbots, such as Apple's Siri, Google Assistant, and Amazon Alexa, are often referred to as 'virtual assistants' or 'virtual agents'. Chatbots have progressed significantly and AI is driving more than just the Language understanding to identify intent. They have the ability analyse the query, formulate and generate responses completely independently based on a particular knowledge base.

Chatbots can interact with members of the public, rather than operating 'behind the scenes'. As such, it is important that sufficient consideration, and where relevant, mitigations, are in place to protect the intended users. Some key considerations include:

- It must be made very clear to users that they are speaking with a chatbot and not a human so that they can make an informed choice as to whether to continue the interaction or not.
- A human-based alternative must be made available, and easily accessible from the page hosting the chatbot, should the user choose to opt out of engaging with the AI, or should they struggle to have their needs met by the chatbot.
- Appropriate guard rails should be put in place to ensure that any Generative AI chatbot is only working with its source information or subset of information to reduce the risk of hallucination or "confidently wrong" responses.

A Data Protection Impact Assessment (DPIA) is required before deploying any chatbot functionality and must be regularly reviewed. This is critical for chatbots accessible to children or vulnerable users, as they may pose high risks to individuals' rights and freedoms. The DPIA should address safeguarding, data sensitivity, and potential harm from inaccurate or inappropriate outputs.

As with any Citizen facing software the data entered by the user may range from, anonymous to sensitive. In the provision of citizen facing platforms the safeguards around where any inputs are sent, how they are used and stored is critical in ensuring customer data is protected. Our impact assessments will ensure some control is in place however, the Service is responsible for understanding it's data flows and transfers.

For further information refer to the Council's Safeguarding Policy and Procedures.

[Corporate Safeguarding Policy 22-25](#)

ChatGPT or other Large Language Models (LLMs) including Copilot

ChatGPT is a Large Language Model (LLM) chatbot created by OpenAI that uses deep learning to generate human-like responses.

LLMs are a type of AI algorithm trained on large collections of text-based data from publicly available sources. These technologies have various possible applications, but they also present certain risks, requiring their use to be managed safely, appropriately, and with accountability.

Officers are to use the LLM technologies and other AI tools, such as Microsoft 365 Copilot, that are accessible via the Microsoft suite of applications made available to them, as the primary option instead of alternative solutions.

The following summarises some of the associated risks in using ChatGPT:

- *ChatGPT has been developed by a US tech start-up and is therefore outside of EU data protection legislation that the Council must follow. Council officers must not input personal data or commercially sensitive information into ChatGPT. If Officers believe that they may have input such data without undertaking impact assessments, they must follow the Council's Data Breach Policy. [Data Breach Reporting Procedure](#)*
- *ChatGPT and other large language model technologies may generate responses that appear plausible but are incorrect.*
- *Information inserted into ChatGPT is not confidential. If chat history is not disabled, query information provided to may become part of its future training dataset.*
- *As with other AI technologies, there is the risk of bias and the production of discriminatory answers. This is exacerbated by LLM technologies that have an extensive*

data source which makes it impossible to completely filter of offensive or discriminatory content.

- *The breadth and extent of the internet data that ChatGPT is trained on is also likely to include copyrighted material, with answers generated without any source references, which poses a potential Intellectual Property or copyright issue for its outputs.*
- *Whilst LLMs do not currently use the information submitted in queries to develop future answers/ responses, this information is available to the AI providers and can therefore be expected to be used for future model training. In addition to this, there is the risk that the AI provider itself could be hacked in the future and thereby made publicly available.*
- *There is the possibility that an LLM system is acquired by different organisations in the future, with different terms of use and privacy policies which might put information submitted into the AI system at greater risk. For these reasons, it is imperative that no sensitive Council information is supplied without proper consideration of the potential risks.*

Submitting personal data to ChatGPT or any other large language model is not permitted. Staff members are provided access to the approved Microsoft 365 Copilot AI tool; consequently, there is no need or justification for utilising alternative AI tools.

Procurement

When officers are engaged in an AI-specific project, the AI technology is often designed and developed externally by a third party. As a result, many AI or AI-related projects involve a commissioning or procurement process.

Officers must follow Cardiff Council policy and guidelines when commissioning and procuring AI technologies.

[Commissioning & Procurement](#)

As an emerging field, the AI marketplace remains underdeveloped, with certain technologies still in pilot phases and associated risks or limitations not yet fully identified. Ultimately, the Council retains responsibility for all outputs derived from these systems. It is essential that officers engage collaboratively with suppliers and ICT to gain comprehensive insight into the risks and considerations addressed during the development of AI solutions.

Officers should also recognise that AI may not always be the default response to new challenges and must conduct thorough assessments of both the risks and limitations inherent in this technology.

Several interdependencies require effective management between Cardiff Council and the supplier, including:

- *The ownership of the data that the AI is trained on.*
- *Transparency regarding the design and assumptions of the algorithm, the extent to which this can be shared between customer and supplier.*
- *Understanding of the legal and ethical accountabilities.*
- *Responsibility and capability for oversight of the technology, monitoring and potential for/ rights around requesting changes.*
- *Integration into existing Council processes.*
- *Compliance with Welsh Language Standards.*

The degree to which these factors are considered should be adjusted based on the project, whether the technology is developed by the Council or externally sourced, and whether AI is the primary focus of the contract or constitutes only a minor component within a broader agreement.

Central government has produced extensive guidelines that will be helpful for any officers procuring an external AI technology.

[Guidelines for AI Procurement](#)

Standards

There are a number of extensive guides and tools, including:

- *Algorithmic Transparency Recording Standard* - [Central Digital and Data Office](#)
- *Data Ethics Framework* - [Data Ethics Framework](#)
- *Ethics, Transparency and Accountability Framework for Automated Decision Making* - [Centre for Data Ethics and Innovation](#)
- *Transparency and Data Protection measures within AI Projects* - [Information Commissioners Office](#)
- *Safer Chatbots - Implementation Guide* - [Safer Chatbots Guide](#)
- *AI Procurement* - [Guidelines for AI Procurement](#)

Welsh Language Standards

Cardiff Council will maintain [guidance on the use of AI tools to facilitate Welsh language services](#) in a way that maintains compliance with our requirements under the Welsh Language Standards.

Key considerations include:

- *Welsh Language Standards* - the overarching principle is that Welsh should not be treated less favourably than English
- *The principle of equivalence of human involvement* – providing services and content in the same way, to the same standard, and with the same level of AI or human involvement regardless of whether the user chooses to access that service in Welsh or English
- *Proofreading* - as with English content produced by AI, it is recommended that official Welsh content produced by AI which represents a Council Communication is carefully proofread by a Welsh speaking colleague a sufficient level of Welsh language skills, or sent to Bilingual Cardiff for [review/user testing](#)
- *Procurement and development* - include criteria relating to Welsh requirements at an early stage and consider steps such as user testing to ensure full functionality

AI for Translation/ Interpretation Services in Other Languages

Staff must ensure any use of AI for translation (the conversion of written text from one language to another) aligns with this Policy and the dedicated AI Document Translation Guidance, which set clear expectations for responsible, lawful, and safe translation practices.

AI translation may only be used for low risk, non-complex content and must never be applied to formal, sensitive, technical, or decision-making documentation.

Staff are required to use only approved tools, follow mandatory two-step quality assurance checks, adhere to strict data handling requirements, and uphold governance standards to maintain accuracy, protect personal data, and safeguard public trust in Council services.

Approved Uses

- Translating **low risk, non-decision making, non-complex** written materials.
- Translating **short, informal correspondence**.
- Using Council approved tools only (Microsoft 365 Copilot, Magic Notes).

Prohibited Uses

- Translating **formal, sensitive, technical, or decision-making documents**
- Translating **right-to-left languages** (Arabic, Dari, Pashto, Kurdish Sorani) without human quality assurance.
- Using **free/open AI platforms** for any translation unless authorised.

[insert Ethical use AI translation guidance doc once approved]

Roles and Responsibilities

The following roles and responsibilities underpin the effective implementation of this Policy.

AI Governance Board

This role provides senior leadership for AI in the Council. The role will:

- Ensure effective governance arrangements are in place for the effective implementation of Artificial Intelligence.
- Oversee the development of policies, procedures and guidance.
- Identifies Council wide AI risks and ensures appropriate action to mitigate risks are agreed and implemented.
- Ensure effective training and staff development is in place.
- Oversee any communications needed about AI.

- Provide updates as required to Senior Management about the delivery AI projects.
- Keep aware of developments in AI and by the regulator - Information Commissioner's Office (ICO) - and proactively communicates them where they are relevant to the Council.

Senior Management will:

- Be accountable for the implementation of AI policies, procedures and guidelines in their service area.
- Take ownership of the implementation of AI in their service area.
- Be accountable for identifying and effectively managing AI necessary for service delivery.

Service Managers will:

- Ensure that staff in their team(s) are aware of policies, procedures and guidance regarding AI.
- Ensure that implementation of AI in their service area complies with policies, procedures and guidance.
- Report breaches in data protection to the Council's Data Protection Officer.
- Identify risks in the implementation of AI in their service area and ensure these are mitigated and/ or escalated as required.
- Ensure that members of staff complete relevant and appropriate training.

Data Protection Officer will:

- Inform and advise the Council and its staff who carry out processing of their obligations pursuant to the UK GDPR.
- Monitor compliance with the UK GDPR and the DPA and with the Data Protection Policy and other Data Protection Policies and Procedures.
- Act as the contact point for the Information Commissioner's Office on all matters relating to data protection and fully cooperate with the regulator.

All Staff (whether permanent or temporary) and others using Council systems or information will:

- Ensure that they are familiar with the contents of this Policy and to ensure the implementation of AI is managed in line with Data Protection policies, procedures and guidelines.

- Make every (reasonable) effort to review and ensure any AI outputs are accurate, avoid discrimination and bias.
- Report breaches of data protection to their manager and DPO via dataloss@cardiff.gov.uk in accordance with the Council's Data Protection Policy.
- Undertake training as appropriate.

Caldicott Guardian will:

- Focus on the management of health and social care information.
- Advise and provide a focal point for service user confidentiality and sharing issues.

Bilingual Cardiff will:

- Advise staff incorporating AI in Council processes and services in relation to how to comply with the Welsh Language Standards
- Compile and periodically update guidance for staff which will

Caldicott Principles

The Council has an appointed Caldicott Guardian - Sarah McGill, Corporate Director People and Communities.

The Caldicott Principles are eight nationally recognised rules governing how confidential health and social care information must be handled. They were formally extended to local authorities with social services responsibilities.

The principles apply whenever we handle information where service users can be identified and expect their data to be kept private, such as names, addresses, health conditions, care records, assessments or safeguarding information. They support safe information-sharing and protect individuals' privacy. They sit alongside UK GDPR and the Data Protection Act.

[Caldicott Guardian role — UKCGC](#)

How We Apply This at Cardiff Council

- **Social Care teams** must document why information is accessed/shared.
- **Only relevant details** should be included in emails, reports or shared files.
- **System access** must be role-based and monitored (no curiosity viewing).
- **Multi-agency partners** (health, police, education) should receive only what they need.
- **Privacy notices** must be clear and up to date.
- **Safeguarding information** should be shared promptly and lawfully where required.

Governance Oversight

Group	Role/ Responsibility
Audit Committee	To provide independent assurance of the adequacy of the risk management framework and the internal control environment. To provide independent review of the Council's governance, risk management and control frameworks and oversee the reporting and annual governance processes. To oversee internal audit and external audit, helping to ensure efficient and effective assurance arrangements are in place.
Corporate Management	Overall approval of Council staff policies, procedures, AI Governance Group (AIGG) terms of reference, formulating and monitoring of Council wide Personal Data processing priorities.
Information Governance & Security Board (IGSB)	To coordinate and oversee Information Governance across the Council. The Group ensures consistent and high standards in the processing of Personal Data in accordance with statutory and legal requirements and monitors the delivery of secure processes that involve personal data.
Caldicott Group	Ensure that the strategic aims and the Data Protection policies, practices and procedures are consistent with the eight Caldicott Principles.
ICT Security & Compliance	ICT management group responsible for ICT Security policy development, advice and approvals.

Training and Guidance

All Artificial Intelligence related policies, procedures and guidance are published on the Council's AI SharePoint workspace and ICT Knowledge Bank and available to all staff. Staff should be made aware of these policies, procedures and guidance.

[AI in Cardiff Council](#)

All staff members are required to complete in the mandatory training sessions and modules provided through the Cardiff Academy learning pool, and must ensure completion of all MetaCompliance courses.

<https://cardiff.learningpool.com/>

Environmental Impact

Efficient use of data can improve delivery, such as by analysing travel routes to lower environmental impact. Yet technology's development, upkeep, and disposal have significant carbon costs. Choices like real-time data feeds, AI, or analytics should be evaluated for their environmental effects.

Review

The regulatory approach of the central government toward artificial intelligence continues to develop. In response, the Council is committed to maintaining a proactive and adaptable stance in formulating policy within this domain, while offering precise guidance to officers regarding the appropriate use of AI. This Policy will be revised as required to reflect changes in national policy frameworks and any new legislation or regulations enacted by the central government.

Any questions regarding this policy should be directed to ICT Service Desk: [ICT Service Desk Self Service Portal](#)