Use “Replace Image” to change this image to your company logo (dimentions may need to be adjusted once changed)

[Company Name] Artificial Intelligence (AI) Usage Policy

Updated: [DD/MM/YYYY]

1. Policy Statement and Purpose

The purpose of this policy document is to provide a framework for the use of Artificial Intelligence (AI) Larger Language Model (LLM) tools (collectively referred to in the rest of this document as ‘AI’) such as ChatGPT, Bard, Bing, Grammarly, or other similar tools by employees, contractors, temporary staff and consultants at [Company Name].

This policy is intended to help colleagues understand our position on the use of AI technologies with in our services. Colleagues currently using or intending to use AI must familiarise themselves with this policy and have a responsibility to maintain transparency in its use. As a result, this policy is designed to ensure that the use of AI is ethical, complies with all applicable laws, regulations and policies, and complements the existing information and security policies.

It is important to note that the pace of development and application of AI, as well as evolving guidance and regulation, is such that this policy will be in a constant state of development and will be reviewed a minimum of every twelve months.

2. What is AI?

AI refers to computer systems capable of performing tasks that would normally require human intelligence. These systems can take many forms, and what is popularly considered as AI is evolving as AI technologies become more embedded in everyday human life. Common forms of AI technology include algorithms and predictive analysis, chatbots and virtual assistants, Machine Learning, remote monitoring tools, smart technologies, text editors and autocorrect, automatic language translation, and facial recognition or detection. It should be noted that these tools can be embedded in other tools – such as email clients or video conferencing tools.

3. Currently Approved AI Tools

At [Company Name], we currently have an approved list of AI tools, which should always be your first place to access AI services. Our approved tools include:

- [list all approved AI tools and any specifications for when and how these should be used if restrictions are included].

4. Opportunities

AI is increasingly being used across industries, including the public sector, for its potential to bring substantial benefits to the way services are delivered. If used safely and appropriately, AI has significant potential to enhance our service for customers, improve how we manage and use data and help us to communicate with and support residents, service users and suppliers more efficiently.

AI has the capability to undertake manual tasks based on large amounts of (usually public) data it has been trained on. For example, it can:

- Produce a range of useful outputs, such as text, audio, images and code without the need for manual inputting. This could apply to the production of minutes, reports or presentations.
- Respond to natural language questions, so any employee and customer can use it, including those for whom English may not be their first or chosen language.
- Understand different types of data, helping organisations to transform large amounts of unstructured data in a variety of formats.

There is increasing evidence that AI can significantly transform the way in which services operate to provide high quality services to businesses and our community. The capability outlined above is only expected to evolve further and provides significant potential to continue delivering services more efficiently at a reduced cost.

5. Information Governance and Data Protection

There is currently no legislation in place that directly refers to the use of AI. However, where an AI system is using or collecting personal data, it will fall within the scope of the UKGDPR and Data Protection Act 2018 (DPA). This could include where personal data is being used to train or test AI, and/or in the deployment of the technology and refers to any personal data held, whether that is in relation to personal data about colleagues or customer information.

The UKGDPR and the DPA gives individuals certain rights where their personal data is being used or created, particularly for automated decision-making. As such, the use of AI carries inherent risks, and these must be considered in the development and use of all relevant AI technologies. When undertaking any activity involving AI, colleagues will review and consider all potential impacts, including UKGDPR and DPA implications, legal compliance, bias and discrimination, security and data sovereignty.

If implementing a new system, or upgrading an existing system, that is likely to involve the use of personal data, colleagues will implement a risk register. If completed at the outset of a project, it can assist in understanding and mitigating any risks.

The Information Commissioners Office has produced guidance on the application of UKGDPR to the use of information in AI systems and the Government has produced a Data Ethics Framework which can similarly be used.

6. Confidentiality

In addition to UKGDPR and DPA implications, colleagues also need to consider the risks associated with the use of confidential, including commercially sensitive, data. Confidential and personal information must not be entered into a public AI tool (such as ChatGPT). This is because the information it may purposefully or inadvertently released it into the public domain, including if the system is breached or hacked. This could lead to potentially facing legal proceedings for breach of confidence or copyright (See section 6). Colleagues must follow all applicable data privacy laws and organisational policies when using AI. For example:

Colleagues must not use an unauthorised AI tool to write a letter to a customer with any personal details in. For example: 'Mr A N Other at 123 Acacia Avenue' as that data will be ingested and kept by the AI for re-use. It would, however, be acceptable for the tool to write any parts of the correspondence which doesn't include personal information.

- Colleagues must not use AI apps on personal phones to record and summarise work meetings, or to use translation services.
- Colleagues must not upload spreadsheets full of customer data for AI analysis.

Confidential or personal information should only be entered into an AI tool that has been built or procured specifically for the enterprise's use, such as Microsoft CoPilot, where the data entered is confined for sole use and use of that tool has been specifically sanctioned for that purpose through the procurement process. So, for example, using Microsoft Teams with a login to transcribe meetings is authorised. However, using a free tool downloaded to a personal phone to transcribe a work meeting is not authorised and could constitute a data breach.

7. Copyright

Colleagues must adhere to copyright laws when utilising AI. It is prohibited to use AI to generate content that infringes upon the intellectual property rights of others, including but not limited to copyrighted material. If a colleague is unsure whether a particular use of AI constitutes copyright infringement, they should err on the side of caution.

8. Data Retention and Security

Colleagues must comply with their department's Data Retention policies for how long any data is retained in a system and, if using personal data, be aware of the obligations in the UKGDPR and DPA about only retaining personal data for as long as necessary to perform the function for which it was obtained.

Colleagues must comply with the data security policies and ensure only those entitled to access the data can do so and, if data is being shared with a third-party provider, that they have adequate security systems in place.

9. Accuracy

AI can completely make up "facts" because they have ingested information from a large amount of data sources, some of which may be fiction. As a result, it is important to fact check any content produced. Furthermore, all information generated by AI must be reviewed and edited for accuracy prior to use. Users of AI are responsible for reviewing output and are accountable for ensuring the accuracy of AI generated output before use/release. If colleagues have any doubt about the accuracy of information generated by AI, they should not use AI without correction.

10. Transparency and Disclosure

In addition to considering UKGDPR and DPA requirements, it is also good practice to maintain the principle of transparency and explainability in the use of AI. This means establishing a clear understanding of the purpose of the technology from the outset. For AI related projects that involve a greater level of interaction with the public or have a potential for having a significant impact on people, colleagues should provide clear information about the algorithmic tools they use, and why they are using them.

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

Note: 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.

11. Procurement

The growth and development of AI technology has a breadth of potential implications for the procurement activities, both where staff are looking to specifically procure an AI technology, and where they are not.

Where colleagues are specifically procuring an AI product, it is likely that the technology will be designed and developed externally by a third party. Colleagues should continue to follow the organizations procurement policy and contract procedure rules with regard to commissioning any procurement, including engaging with the IT team early in the process, but will need to be aware of the unique challenges associated with AI technologies. As a burgeoning field, the AI marketplace is not yet fully developed, meaning that in some areas, available technologies may still be in pilot stage and the risks or limitations not fully understood. Colleagues will be expected to work with the chosen supplier to fully understand the risks and considerations that have been made in the AI's development, as ultimately responsibility for the outputs will sit with the business. Staff should also ensure that they undertake due diligence when selecting a supplier, even if the supplier pool is small. When developing such a project, staff should keep in mind that AI cannot be assumed to be the default solution to the emerging needs and challenges that are faced and should therefore carefully consider the risks and limitations of this technology.

There are a number of interdependencies that will need to be managed between the user 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 processes.

The level of consideration of these factors should be tailored to the specific project, the extent to which it is a -designed technology (as opposed to an already existing product or one to be designed externally), and whether the entire contract concerns AI or if it is a small part of a wider contract.

12. Social Impact and Equality

There is under a legal duty to comply with the Public Sector Equality Duty (PSED) under the Equality Act 2010. This means that when developing using or procuring AI technologies the business needs to consider the potential impact on people with protected characteristics. This consideration may be made and evidenced though an Equality Impact Assessment (EIA). Colleagues must be aware of how the use of AI may impact different groups of people in different ways as it may have inherent social bias through historical structural inequalities or have been trained on stereotypes, which can then become replicated and amplified in its outputs through AI. It may have inappropriate cultural values or display sensitive content and therefore AI must not be allowed to solely determine which customers should have access to services; Humans must be involved in such decision-making where needed, and there must be an appeal processes for any automated or AI-informed decisions.

In order to mitigate these risks, data sources that will be used to train AI, as well as data sources that the technology will be using to make its analysis or predictions, should be assessed for potential unconscious bias or discriminatory outcomes at the start of an AI project. If potential bias is identified, an alternative data source should be used or the bias should be trained out of the tool before it is used.

13. Digital Exclusion

Whilst less applicable to AI technologies used internally only, the impact of digital exclusion may be relevant to technologies intended to be used by customers or service users. Mitigation of the impact of digital exclusion is important and that the use of AI aligns with this approach. Whilst new technologies can be effectively utilised to support digital inclusion, for relevant technologies, the impacts should be considered as part of the EIA process to ensure that alternatives are in place for those who experience digital exclusion and are therefore unable to access the benefits of the AI technology.

14. Ethical Use

AI must be used ethically and in compliance with all applicable legislation, regulations and organisational policies. Colleagues must not use AI to generate content that is discriminatory, offensive, or inappropriate. If there are any doubts about the appropriateness of using AI in a particular situation, colleagues should consult with [line manager/any relevant job titles].

15. Data sovereignty and protection

Colleagues must be clear who owns the data being used, particularly if procuring a product from a third party. They should ensure it retains ownership of the data and complies with the UKGDPR and DPA if it is intended that the third party are going to be processing the Data on the business's behalf. Colleagues are also required to know where the data is being stored, as there are restrictions in the UKGDPR and DPA on ensuring any personal data is only stored within those countries with suitable Data Protection policies.

16. Training and Support

In order to support this policy, additional guidance for colleagues will be developed via the website or internally, supported by updates to the security awareness training packages. AI as a skillset is recognised as a significant future need for the organisation and the future plan will be to identify suitable, accredited courses to establish a core number of colleagues specifically trained in the use of AI.

17. Compliance

Any violations of this policy should be reported to their line manager. Failure to comply with this policy may result in disciplinary action, in accordance with Human Resources policies and procedures.

In the event of a breach caused by a third party, the business will consider immediately suspending the staff in addition to the provisions within our Data Protection policies.

18. Review

In line with the principles of continuous improvement, this policy will be reviewed a minimum of every twelve months and updated as necessary to ensure continued compliance with all applicable legislation, regulations and organisational policies. Feedback mechanisms will be established for each system implemented to gain input from stakeholders and identify opportunities for improvement.

Created/Updated By	[Full Name, Job Title]		
Approved By	[Full Name, Job Title]		
Version	Version [0.0]	**Date**	[DD.MM.YY]