Artificial Intelligence Corporate Policy DPIA

The DPO can assist with items in purple in this document.

Submitting controller details

Name of controller	Spelthorne Borough Council
Subject	Artificial Intelligence Corporate Policy
Name of controller contact (staff member completing)	Sacha Bailey

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Spelthorne Borough Council are seeking to develop and implement a corporate policy for artificial Intelligence (AI). This policy review is part of a broader Council project that is evaluating how SBC polices are currently managed within our software systems.

An effective corporate AI policy will seek to address several critical aspects to ensure responsible and ethical use of AI technology across the organisation. The policy will outline the following:

1. What is Artificial intelligence (AI)?
2. What are the risks of AI?
3. Decision Making
4. Language Models
5. What Does this mean for staff?

A Data Protection Impact Assessment is required because there are data privacy and security implications involved when deploying AI. Given AI's reliance on data, the policy will need to consider information governance, data protection, transparency, equalities, digital exclusion, and types of AI technology being used e.g. chatbots, copilot, generative AI. A DPIA is required to ensure responsible AI deployment and compliance with data protection regulations.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Data Collection: Data will be collected from various sources including websites (e.g. chatbots, Co-Pilot), individual apps for computers, plug-ins for websites, new features on computer software, external databases, and API's.

Data Use: Data extracted from AI tools will be used to support individual tasks such as creating images and documents, generating text or content for reports, emails, presentations, and customer service communications. Data entered can also be used to quickly find sources of information and break down complex topics into easily understood information.

Data Storage: Data about your interactions with GenAI is stored within the Microsoft 365 service boundary, and this includes prompts and responses from the AI tool.

Data Deletion: Interactions with AI tools and applications can be deleted from the user's interaction history. Data will be deleted when no longer necessary for the specified purposes. Deletion procedures will follow data retention policies.

Data Sources: Data can come from various sources such as website content, third-party data providers (e.ge. API's) and user-generated content.

Data Sharing: Generated data may be shared with internal teams, third party suppliers, regulatory authorities.

High Risk

Profiling: Creating profiles based on individuals' data raises privacy concerns. Consideration must be given to the safeguarding of individuals privacy.

Data collection and fairness: Aggregating and anaylsing personal and sensitive data on a large scale can infringe on privacy. AI systems that learn from biased data may perpetuate or amplify existing biases, leading to unfair treatment. Local Authorities have a duty to adhere to the Public Sector Equality Duty. Confidential and personal data must not be entered into a GenAI tool, as information may enter the public domain.

Inferences about individuals or groups: AI can infer sensitive information from seemingly innocuous data and a consideration will need to be given to privacy rights. For these reasons, AI tools should not be used for decision making and a meaningful review by an officer should be undertaken before making a decision.

Transparency and Accountability: Transparency and accountability are compromised if the user does not clearly state that the output of GenAI has been significantly used in their work. The author must take responsibility for AI generated content, and any content must be reviewed by the author for accuracy and revised/edited where necessary.

Security: Inappropriate access, unauthorised or unlawful processing and undetected security vulnerabilities can be an issue with AI. Security risks should be assessed and documented to ensure the AI tools being used are as safe as possible.

These activities are considered high risk due to the nature of the data involved and their potential impact on privacy and individual rights.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Data Nature: The nature of the data includes text, images, video, audio, and software code. Currently, users will not be allowed to enter personal data into AI tools and applications.

Special category or criminal offence data: The Council staff will not use AI tools to enter personal data and so the scope of the processing will not include special category data or criminal offence data.

Level of data collected and frequency: AI tools and applications are used daily by Council staff. The level of data collected will consist of AI generated content for documents, emails, and presentations. AI generated output will also act a source to explain complex information.

Retention of Data: Interactions with a GenAI tool will be deleted from the interaction’s history. Data will be deleted when no longer necessary for the specified purposes. Deletion procedures will follow data retention policies.

Number of individuals affected: All Council staff will be impacted by the use of AI. There should be minimal impact on residents as personal data will not be allowed to be entered into AI tools. The use of GenAI tools will affect how emails, documents and images are constructed.

Individuals affected and geographical area: Council staff who use GenAI will be affected. Residents will not be individually affected as users will not be allowed to enter personal data into AI tools.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Relationship Nature: although no personal data will be entered into AI tools, the Council have a responsibility to adhere to the public sector equality duty. Users of AI tools will have control over what information is entered into a GenAI tool.

Data Control: Individuals will have little control over the council's use of GenAI, however the staff must use GenAI responsibly and ethically.

User expectations: Most individuals understand that as Artificial Intelligence becomes more widely used, the Council will use AI to improve operations, decisions, and services. Council's need to be transparent with residents about their use of GenAI, particularly if used in public facing.

Children's Data and Vulnerable groups: Users will not enter children's data or the information of vulnerable groups into AI tools.

Prior Concerns and Technology: There has been some concern around AI especially regarding the use of personal data, privacy issues, bias and profiling and software security. The recent launch of generative AI tools, such as Chat GPT, Co-pilot and Google Bard, are free and user friendly; and can almost instantly respond to questions and prompts by generating original text, images, data, code and sounds, hence the term ‟generative AI”.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Primary Objective: The primary objective is to use GenAI for work-related purposes for tasks such as generating text or content for reports, emails, presentations, images and customer service communications.

Intended effects on individuals: The use of GenAI will assist users with creating comprehensive and well produced documents, images and reports, that are easy to understand. GenAI also acts as a source of information, which is a useful tool to help expand staff knowledge and skillsets.

Benefits: Improve service delivery, as reports and documents composed within a timely manner. Increased productivity in general tasks e.g. writing emails, summarising content, and producing reports. An additional benefit is that GenAI can be used to explain complex tasks.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Consultations will take place with Subject Matter Experts (SME's) such as the Data Protection Officer, ICT Manager and Legal.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Since at this stage of the project no personal data is to be used in connection with AI there is no need to determine a lawful basis for processing.

The Lawful bases for processing are:
Legal obligation: the processing is necessary to comply with the law.
Public task: the processing is necessary to perform a task in the public interest or for official functions.
Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party.
Vital interests: the processing is necessary to protect someone's life.

The following categories of personal data are defined as being special category and require identification of an additional lawful basis:
racial or ethnic origin,
religious or philosophical beliefs,
genetic data,
sex life or sexual orientation data,
political opinions,
trade union membership,
biometric data,
health data.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
See DP risks to consider template_AI Policy.xlsx (sharepoint.com)	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	Sacha Bailey	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Sacha Bailey	If accepting any residual high risk, consult the ICO before going ahead

DPO advice provided:	By comments in document and discussion	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: DPO advice was not to use AI for personal data as a baseline. This can be reviewed on a case-by-case basis however considerable data protection (and other) work will be needed before any personal data is entered into any AI software tools.		
DPO advice accepted or overruled by:	Accepted by Sacha.	If overruled, you must explain your reasons
Comments: To be reviewed regularly.		
Consultation responses reviewed by:	N/A	If your decision departs from individuals’ views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	Project Team, DPO.	The DPO should also review ongoing compliance with DPIA