

USE OF PERSONAL DATA IN AI MODELS POLICY (UK AND EU)

CONTENTS

CLAUSE

1	About this policy	2
2	Who does this policy apply to?	2
3	Who is responsible for this policy?.....	2
4	Scope of the policy	3
5	Procurement from external providers	3
6	Data minimisation and exceptions process.....	4
7	Model monitoring and project completion.....	5
8	Design principles to address model bias and promote fairness	5
9	Transparency, explainability and security	6
10	Training, audit and monitoring	7
11	Breach of this policy	7

Annex A

Key Terminology	8
-----------------------	---

1 About this policy

- 1.1 The use of AI is transforming the way individuals are working. Informed and responsible use of AI has the potential to foster innovation and transform organisations. With these potential benefits come potential risks, including the inappropriate use of personal data in AI models which can have serious impacts on individuals and society, as well as legal, regulatory and reputational risks for organisations.
- 1.2 The purpose of this policy is to ensure the ethical and responsible use of personal data when procuring, developing and deploying AI models at the University of Kent ("we", "our", "us"). This policy will help the University remain compliant with laws including the UK GDPR, the EU GDPR and the EU AI Act, and align with our *Principles for Responsible and Effective Use of Artificial Intelligence*.¹
- 1.3 This policy does not form part of any contract of employment or contract to provide services, and we may amend it at any time.

2 Who does this policy apply to?

- 2.1 This policy applies to all staff, employees, officers, consultants, contractors, volunteers, interns, casual workers and agency workers (collectively referred to as 'staff') and students (in so far as students have access to University personal data²) ("you", "your") who are considering the use of personal data in the training, development, deployment or use of an AI model. Where students are instructed to use personal data by their course tutor, the responsibility for compliance lies with the course tutor.

3 Who is responsible for this policy?

- 3.1 The Executive Group has overall responsibility for the effective operation of this policy and for ensuring effective training for staff is available and compliance monitored. The Audit Committee will provide governance oversight on behalf of Council. The Executive Group has delegated responsibility for overseeing its

¹ <https://student.kent.ac.uk/studies/using-generative-ai-in-your-studies/ai-use-guidelines/our-ai-principles>

² 'University personal data' includes personal data collected from human participants in research projects. See full definition of personal data in Annex A 'Key terminology'.

implementation to the University Secretary. Questions about the content of this policy or suggestions for change should be reported to the Data Protection Officer.

- 3.2 In order to address evolving uses and understanding of AI, this policy is reviewed at least annually by the Data Protection Officer (or similarly qualified member of Governance, Assurance and Legal Services), consulting with relevant committees as necessary.

4 Scope of the policy

- 4.1 This policy applies to any use or potential use of personal data when procuring, developing and deploying AI models for University purposes.
- 4.2 This policy supplements and should be read in conjunction with our other policies, procedures and guidance in force from time to time, including without limitation our:
- (a) Data Protection Policy;
 - (b) Data Breach Policy;
 - (c) Data Protection Code of Practice;
 - (d) Equality, Diversity and Inclusion Policy;
 - (e) Ethics Code;
 - (f) Information Security Policy;
 - (g) Intellectual Property Policy;
 - (h) IT Regulations;
 - (i) Procurement manual;
 - (j) Risk Management framework;
 - (k) Respect at Kent.

These are available on the **Governance** pages of the University's website.

5 Procurement from external providers

- 5.1 If you intend to procure AI models or systems from an external service provider, you must follow the University's procurement process and contact the ITS Digital

Enablement Team so that technical aspects and licencing terms can be reviewed in relation to relevant policies.

- 5.2 The Procurement process must also include appropriate due diligence on the provider to ensure any data protection risks, including those relating to the use of personal data in the model, are fully understood before engagement. A Due Diligence Questionnaire Template is available on **SharePoint** or from the Data Protection Office and this should be sent to the prospective service provider to complete.
- 5.3 Any model that has been developed by a service provider using personal data or that contains personal data will be subject to this policy.

6 Data minimisation and exceptions process

- 6.1 **The default position is that you should not use personal data to develop, train, test, operate or use any AI models.** This use may conflict with data protection laws, including the requirement to minimise the processing of personal data under the UK GDPR and the EU GDPR and other restrictions.
- 6.2 Exceptions to the default rule in paragraph 6.1 may be approved by the Data Protection Officer on a case-by-case basis. Before seeking an exception, you should consider whether personal data is necessary to support your proposed use case or whether you could use anonymised data as an alternative.
- 6.3 If you decide you would be able to achieve your use case objectives by using an anonymised or de-identified dataset, you must still consult with the Data Protection Officer before proceeding. They will need to verify the anonymisation or de-identification process has been carried out satisfactorily before giving their approval. You should complete a ***DPIA screening questionnaire*** and send it to **dpomatters@kent.ac.uk**. This approval may be subject to the completion of a data protection impact assessment (DPIA).
- 6.4 If you decide you need to use personal data for your use case, and the anonymisation or de-identification of data would not be appropriate, you must contact the Data Protection Officer who will be responsible for reviewing your proposal, involving any other relevant stakeholders, and advising you on your DPIA. You will be required to provide input and support to the review team so they can

form a complete understanding of how personal data will be processed, including any potential impacts on individuals, and what controls might be put in place to mitigate any risks.

- 6.5 Following completion of the DPIA, the Data Protection Officer may grant approval to proceed if the use of personal data is absolutely necessary, but this is likely to be subject to strict controls being put in place.
- 6.6 Following approval, the **Project Lead** designated by the Information Asset Owner (Head of School or Department) will have responsibility for overseeing the implementation of the controls for the duration of the project and reporting on the progress of the project, as required by the DPIA.
- 6.7 The Data Protection Office will maintain a list of all AI and Generative AI applications that have been approved together with details of the approved use case. This is available on **SharePoint**.

7 Model monitoring and project completion

- 7.1 If a personal data use case for AI has been approved by the Data Protection Officer, the Project Lead must carry out monitoring of the model's performance to ensure it remains compliant with the approved use case at all stages of the model lifecycle. If there is any risk that the model no longer performs consistently with the approved project use case, the Project Lead must immediately report this to the Data Protection Officer.
- 7.2 On completion of a project, the Project Lead must immediately inform the Assurance & Data Protection Office and work with them as required, including on the process of securely deleting any personal data used for the project that is no longer required.

8 Design principles to address model bias and promote fairness

- 8.1 If a personal data use case for AI has been approved by the Data Protection Officer, the Project Lead is responsible for ensuring activities align with the University's EDI Policy when designing and deploying AI models to eliminate or mitigate negative impacts on individuals. You must adhere to the following model design principles when designing models to eliminate or mitigate negative impacts on individuals:

- (a) Proactively address bias and discrimination risks by:
 - (i) adopting or obtaining evidence of a human-centred approach to AI model development;
 - (ii) evaluating your proposed model training data for accuracy, representativeness, reliability and relevance to ensure it reflects the population or groups the model will impact;
 - (iii) conducting mapping exercises to understand the potential outcomes of the model's decisions for different groups and assess whether these align with our Ethics Code³;
 - (iv) considering techniques to mitigate bias and discrimination, including balancing training data to account for underrepresented population subsets, modifying the dataset or learning process to overcome past discrimination and establishing criteria and accountability for labelling data involving protected characteristics.
- (b) Prepare training data appropriately to promote fairness by:
 - (i) establishing clear criteria and lines of accountability for labelling data that involves protected characteristics or special categories of personal data;
 - (ii) considering the use of a second human labeller to review labelling and ensure consistency; and
 - (iii) using or obtaining evidence of privacy-preserving techniques to anonymise, de-identify or pseudonymise personal data.
- (c) Test and monitor outputs and guide the user to ensure the inclusion of human intervention.

9 Transparency, explainability and security

- 9.1 You must provide clear and meaningful explanations to individuals if personal data will be processed using AI under an approved use case in accordance with the University's Data Protection Policy and in order to meet AI transparency

³ <https://www.kent.ac.uk/governance/downloads/documents/ethics-code.pdf>

requirements under applicable national Codes⁴ or (where applicable) as required under the EU AI Act⁵.

- 9.2 You must consider the cybersecurity and information security aspects of using personal data in models to ensure that your proposed use complies with the Information Security policy, IT Management Policy and IT Regulations, and contact the ITS Digital Enablement team for guidance.

10 Training, audit and monitoring

- 10.1 The University is required to ensure you have undergone adequate training to enable you to comply with data protection and other relevant legal requirements. The University must also regularly test our systems and processes to assess compliance including monitoring.
- 10.2 You must undergo all mandatory data protection training and complete AI-literacy training where you are directly involved in AI deployment.
- 10.3 You must regularly review all the systems and processes under your control to ensure they comply with this policy and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.
- 10.4 This provision operates alongside the University's right to conduct monitoring for security purposes under the *IT Regulations and Information Security Policy*.

11 Breach of this policy

- 11.1 Breach of this policy may, where appropriate, result in disciplinary action. Staff who fail to observe this policy may be subject to Statute 7 and associated Ordinances (e.g. Conduct). Students who fail to observe this policy may be subject to the Student Discipline Procedures.
- 11.2 You are required to co-operate with any investigation into suspected breach of this policy. This may involve providing us with access to AI systems where necessary.
- 11.3 You must report any breach of this policy immediately to the Data Protection Office.

⁴ <https://www.gov.uk/government/publications/ai-playbook-for-the-uk-government/artificial-intelligence-playbook-for-the-uk-government-html>

⁵ https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689#art_50

ANNEX A Key terminology

We set out below some common terms used in relation to AI, data protection and privacy and what they mean:

- AI stands for Artificial Intelligence.** The definition of an AI System adopted by OECD countries states: “An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.” The EU AI Act⁶ defines an AI system as “a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments”
- Direct identifier.** Data that alone or in combination with other data can directly identify an individual. Examples include an individual's full name, email address, telephone number, National Insurance number and passport number. (See ‘Personal data’ definition.)
- Enterprise System.** The integration of advanced AI enabled technologies and techniques within large organisations to enhance business functions. Within the University of Kent this includes approved AI and approved gen AI systems that are closed to Kent only and therefore covered by a data processing agreement.
- Generative AI.** This refers to a type of AI which can be used to create new content (for example, text, code, images, videos or music) (referred to as the output). The AI uses machine learning algorithms to analyse large datasets.
- GPT.** This is short for "gen pre-trained transformer", which is a type of LLM that uses deep learning to produce natural language texts based on information

⁶ (EU) 2024/1689 Article 3(1)

requested in the input. ChatGPT is an example of a GPT model which can be used to generate text.

- **Hallucination.** LLMs can produce outputs which may initially appear to be believable but are in fact highly inaccurate or fabricated. This is known as a hallucination.
- **Indirect identifier.** Data that, when combined with other data, can lead to the indirect identification of an individual. Examples may include non-specific attributes such as birthdate, gender, postal code and occupation. The more indirect identifiers present in a dataset, the more likely that an individual's identity can be inferred. (See 'Personal data' definition.)
- **Large language models (LLMs).** LLMs are a type of GenAI that can generate human like text in response to a prompt. They use deep learning techniques and massive data volumes to generate a response.
- **Machine learning (ML).** ML is a subset of AI that enables computers to learn and improve without being explicitly programmed. ML focuses on developing computer programs that can learn trends and patterns from data to make predictions or optimisations. ML includes reinforcement learning, supervised learning and unsupervised learning.
- **Model.** A quantitative method, system or approach designed by humans to solve tasks. It processes input data to generate insights that can be put to a range of uses including decision-making and making predictions. A model typically has three components: the data input component (including assumptions), the processing component which transforms the input data into estimates, and the results component which presents the estimates in a useful manner for the user.
- **Model monitoring.** The process of tracking the performance of AI/ML models in production environments. It could involve monitoring of data drift, concept drift, model assumptions, bias, explainability and other expectations from the model.
- **Personal data.** Any information identifying a living individual or information relating to a living individual that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special categories of personal data and

pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

- **Prompts.** These are the inputs or queries that a user provides to generative AI applications to receive the required output. Prompts can be used by the application to further train an LLM.
- **Special categories of personal data.** The subset of personal data the processing of which is either prohibited or requires additional protection under the UK GDPR or the EU GDPR (or both), including data revealing a data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data, health and sex life or sexual orientation.

Document control

Document title: Use of personal data in AI models policy

Version	Author/feedback	Change	Date	Next Review
0.1	AD (Assurance)	Draft Policy created	06.06.25	
0.2	DPO	Minor amendments to definitions and policy section	09.06.25	
0.3	AD (Assurance)	Further minor amends	05.09.25	
0.4	AI Policy Group	Minor comments/feedback	24.04.26	
0.5	DPO	Comments actioned and minor amends to formatting, order and breach of policy clause.	27.05.26	08.06.27

Approval

Version	Reviewing/Governing Body	Review/Approval Date
1.0	EG and Audit Committee	08.06.26