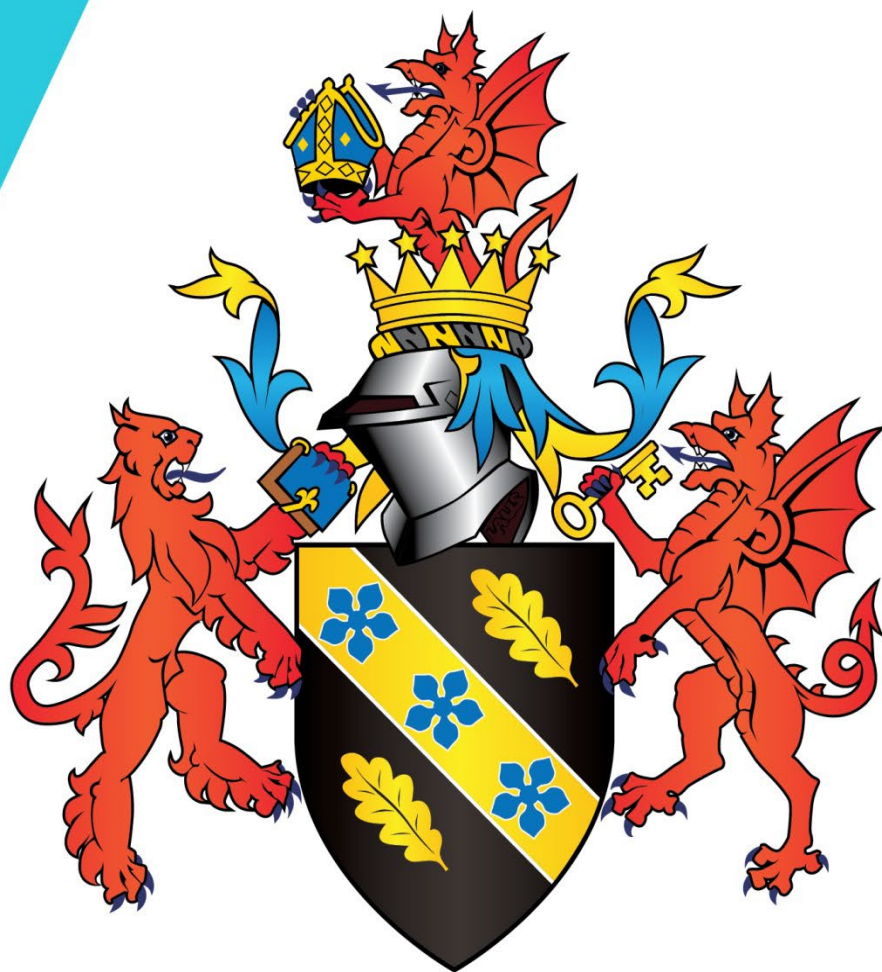




Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David



UWTSD

Generative AI and AI Systems - Guidance for Staff

Contents

1. Definitions	3
2. Guidance	4
3. Data - Guidance on the processing of data using Generative Artificial Intelligence.....	10
4. Use of AI Agents	11
5. Use of Generative AI in Research.....	12
6. Legal perspective	13
Appendix 1	15

Guidance and advice for staff on the use of Generative Artificial Intelligence (AI) and AI Systems

1. Definitions

1.1 What does this guide cover?

This guide covers the use of Generative AI and wider Artificial Intelligence (AI) systems and tools by university staff. It provides guidance on the benefits, limitations and responsible use of AI, including data protection, legal and ethical considerations.

It also explains how staff should assess proposed AI use cases, including when use can proceed within existing guidance, when advice should be sought, and when a formal AI Tool Request is required. The guide also provides information on some of the AI tools and solutions available to staff, how to access supported services, and links to further resources and training.

1.2 What does this guide not cover?

This guide does not cover any learning & teaching specific guidance for staff – these elements (including elements like ethics and assessments) can be found on the [University's learning & teaching guidance](#) located on Moodle which is specifically around AI within the Learning and Teaching context.

1.3 What is Generative AI?

Generative AI refers to advanced artificial intelligence systems designed to create new content, including text, images, music and more, by learning from vast datasets. These systems use machine learning, especially deep learning techniques, to understand patterns, styles and structures of human-made content.

Unlike traditional AI, which focuses on analysis and prediction, Generative AI excels in producing novel outputs, often requiring minimal human input. It has applications across various fields, such as art, entertainment, design and automation, offering innovative solutions and enhancing creativity. However, it also presents ethical and operational challenges, including concerns over copyright, authenticity and the potential for misuse. UWTSD staff have access to Copilot from Microsoft as the recommended generative AI solution, with more details on this within this guidance.

1.4 What is GPT?

GPT (Generative Pre-trained Transformer) is a transformative AI technology, designed to generate text that mimics human writing. You have probably heard of the first and most well-known GPT model: ChatGPT. It is a cornerstone of Generative AI, trained on extensive internet text to perform tasks like writing, answering queries and translation. Its architecture excels in processing data sequences, making each GPT iteration more adept at producing coherent, contextually relevant responses.

There are differing versions of Open AI's GPT that you may see when looking into Generative AI, they essentially mark the evolution of this technology, with each new version bringing improvements in understanding, context awareness and output quality. Starting from GPT-1, each subsequent version (GPT-2 up to GPT-5 and beyond) has been significantly larger and more capable, offering more sophisticated responses and a broader understanding of language. Microsoft's Copilot also takes advantage of the latest OpenAI GPT model.

Other major Large Language Models (LLMs) include Claude (Anthropic), Gemini (Google DeepMind) and LLaMA (Meta). Most now offer enterprise-grade versions that include privacy controls, opt-outs from training data use, and integration with institutional systems. There are others too, with lots of [information available online](#) comparing the different offerings.

1.5 What can they do and how they can be helpful?

Generative AI offers transformative benefits for both the workplace and educational environments, fostering creativity, efficiency, and innovation. For staff, incorporating Generative AI into daily tasks and learning processes can significantly enhance personal productivity. Some of the benefits are outlined below:

- **Automated Administrative Tasks:** Generative AI can automate routine tasks such as scheduling, email correspondence, and document management.
- **Research Capabilities:** It aids in data analysis, literature reviews, and hypothesis generation, accelerating the pace of research and discovery (notwithstanding ethical issues associated with research usage around sensitive information).
- **Creative Content Generation:** For marketing and communications, Generative AI can produce innovative designs, write compelling content, and create engaging multimedia materials.
- **Personalised Learning Materials:** Facilitates the creation of customised learning resources to address diverse student needs and learning styles.

2. Guidance

2.1 All staff

The University does not wish to stop university staff in utilising Generative AI technologies as part of their work. However, it is crucial that any work produced with the aid of AI is not misrepresented as the individual's sole original creation. Generative AI can be considered a valuable supplementary tool in the creation of such work, enhancing both creativity and efficiency.

The global academic and professional communities continue to explore and identify several applications for these emerging technologies, emphasising the importance of adhering to ethical standards in their use.

Please read this guidance document so that you can fully understand both the positives and negatives of using Generative AI, so that you can make informed decisions about its potential use cases.

2.2 Academics and staff engaged in and supporting learning & teaching and research.

Please utilise the [University's existing guidance](#), located on our Moodle page, which is specifically around AI within the Learning and Teaching context.

The University has been running a number of training opportunities for staff and students on the above, with further information on these sessions available via the Staff bulletin, on the [AI Learning Community site](#) and searchable via the [DigiCentre Resource Finder](#).

Section 5 contains specific guidance around the use of generative AI within research.

2.3 How secure are generative AIs to use?

The level of security, privacy and data protection provided by Artificial Intelligence (AI) systems varies significantly between different tools, providers and licence types. Staff should not assume that information entered into an AI system is private, confidential or protected simply because the service requires a login or is a paid product.

The University recommends that staff use University-supported and approved AI tools wherever possible. For example, staff using Microsoft Copilot should sign in with their UWTSD credentials so that their use is covered by the University's Microsoft 365 security, data protection and compliance arrangements.

Particular care should be taken when using publicly available AI services, free versions of commercial AI products, or services accessed through personal accounts or subscriptions. Information entered into these services may be stored, processed outside the University's control, used to improve the provider's services or models, or otherwise handled in ways that are not appropriate for University information.

Staff should therefore not enter personal, confidential, sensitive, restricted, copyrighted or other protected University information into an AI system unless the system and proposed use are permitted under this guidance or have otherwise been appropriately approved by the University. Further guidance is provided in Sections 2.4 and 3.

The fact that an AI product offers enhanced privacy settings, a paid subscription or an option to prevent data being used for model training does not, on its own, mean that the product is approved for university use. Staff should also avoid making their own assessment of whether a new AI service is sufficiently secure for institutional use where University information, systems or services are involved.

Where staff wish to use AI for low-risk activities involving publicly available or non-sensitive information, this can normally proceed in accordance with this guidance. Where the proposed use involves University data, personal information, integration with university systems, decision-making, procurement or the introduction of a new AI tool or service, staff should follow the risk-based approach outlined in Section 2.4 – Using AI Safely: Use Cases and When to Seek Guidance.

If you are unsure whether an AI tool or proposed use is appropriate, seek advice before entering University information or proceeding with the activity.

2.4 Using AI Safely: Use Cases and When to Seek Guidance

2.4.1 What is an AI Use Case?

An AI use case refers to any activity where artificial intelligence is used to:

- **Generate content**
(e.g. drafting text, creating images, generating code, summarising documents)
- **Analyse or interpret data**
(e.g. identifying patterns, summarising datasets, producing insights)
- **Support or influence decisions**
(e.g. recommendations, automated responses, prioritisation or triage)

AI use cases can range from low-risk, everyday productivity tasks to more complex or higher-risk applications involving data, systems, or decision-making.

The use of AI tools such as Microsoft Copilot for general tasks (e.g. drafting emails or summarising documents) is considered an AI use case but does not automatically require further approval or escalation.

2.4.2 Using AI Safely – A Risk-Based Approach

The University adopts a proportionate, risk-based approach to the use of AI.

In most cases, staff can use AI tools within the guidance provided in this document. However, there are situations where additional care or formal review is required.

The following model provides a simple way to determine what action is needed.

Green – Proceed

You can proceed without further action where:

- You are using an approved AI tool for low-risk purpose (e.g. enterprise Microsoft Copilot or systems aligned with section 2.3 and/or Appendix 1 of this guidance)
- You are working with:
 - Publicly available information
 - Non-sensitive data
- The AI is being used for general productivity or support tasks
- No new system, integration, or service is being introduced

✓ No further action required

✓ Continue to follow this guidance and apply professional judgement

Routine use of ordinary personal data within an approved University enterprise AI service, such as Microsoft Copilot accessed with UWTSD credentials, does not automatically require formal review where there is a legitimate business need, the data used is limited to what is necessary, and normal University data-protection requirements are followed.

Amber – Seek Advice

You should seek guidance where any of the following applies:

- You are unsure about the data being used (e.g. potential for re-identification)
- The dataset is not yet public, or contains unpublished or third-party data
- The AI output may influence decisions or outcomes
- You are considering using an AI tool that is unfamiliar to you or whose status under university guidance is unclear.
- You are unsure whether your use complies with:
 - Data protection requirements
 - Research ethics
 - Copyright or licensing

In these cases, you should seek advice from:

- Digital and Information Services
- Data Protection team (if data-related)
- Research governance (if research-related)

This is intended to be a light-touch check, not a formal approval process.

Red – Formal Review Required

You must follow the University's AI Tool Request Process where any of the following applies:

- The AI tool or system will involve higher-risk processing of personal data, including:
 - Special category or sensitive data
 - personal data processed in an AI system that has not already been approved by the University for that type of use
 - personal data used to make, support or significantly influence decisions affecting students, staff or services
 - large-scale, unusual or particularly sensitive processing of identifiable individuals

- personal data used through new integrations, agents or automated workflows that have not previously been approved
- You are proposing to:
 - Procure, licence, deploy, implement or formally introduce a new AI tool, system or platform for university use.
 - Integrate AI with existing University systems (e.g. Moodle, Microsoft 365, APIs)
- The AI system may:
 - Make or influence decisions affecting students, staff, or services
 - Generate outputs that may materially affect or be used to make, support or significantly influence decisions about identifiable individuals.
- There are:
 - Contractual, legal, or intellectual property considerations
 - Potential reputational risks to the University

In these situations, you must complete the AI Pre-Screening Form and follow the AI Tool Request Process (see below).

This ensures:

- Compliance with GDPR and data protection law
- Appropriate technical and security review
- Alignment with University policies and standards

2.4.3 AI Tool Request Process

Where a formal review is required, staff must follow the University's AI Tool Request Process.

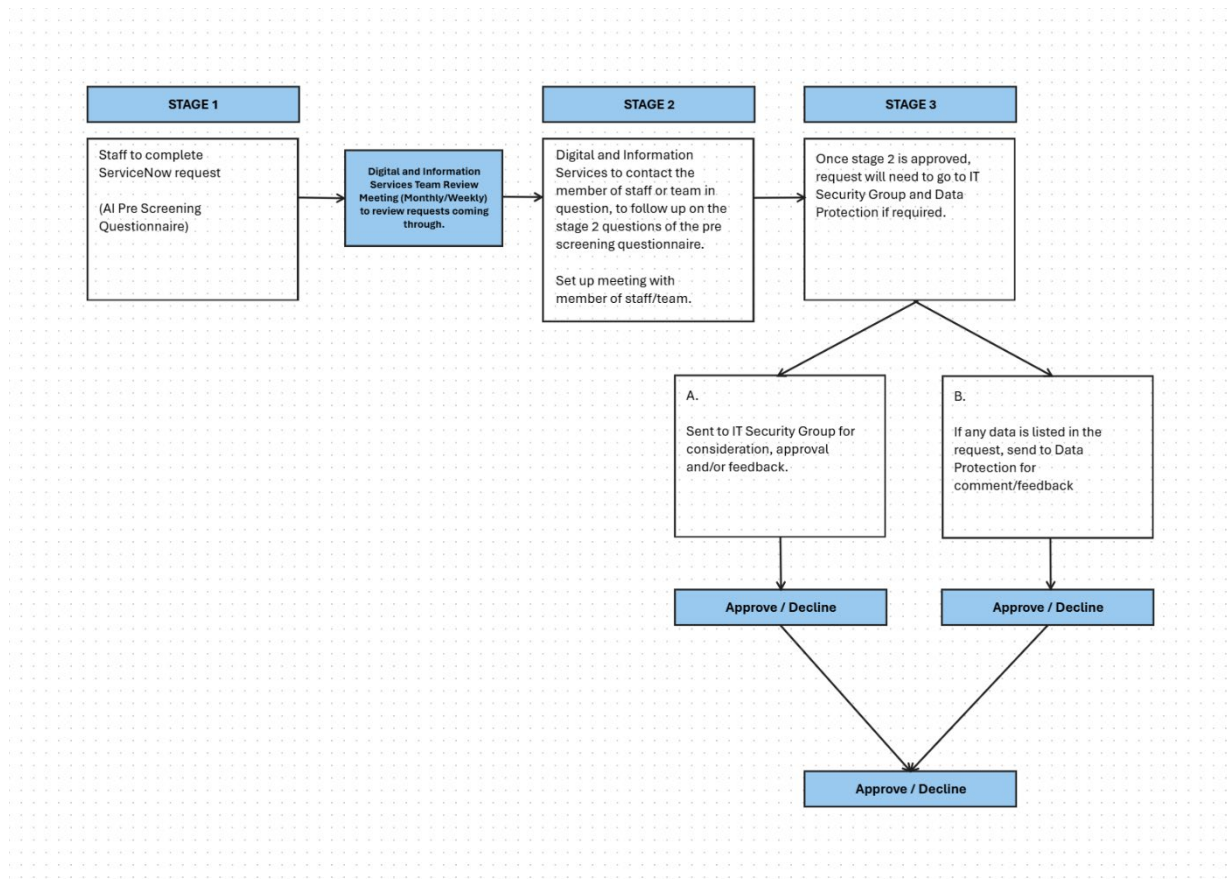
This process includes:

- Completion of an AI Pre-Screening Form
- Review by Digital Services
- Additional checks where required (e.g. Data Protection, IT Security, Procurement)

The process is designed to:

- Protect staff, students, and University data
- Ensure safe and compliant use of AI technologies
- Avoid duplication of tools and unnecessary risk

Link: [ServiceNow - AI Tool Request](#)



2.4.4 Key Principles

When using AI, staff should:

- Apply professional judgement and act responsibly
- Follow existing guidance on:
 - Data protection
 - Academic integrity
 - Research ethics
- Seek advice where unsure
- Escalate only where necessary

The aim of this approach is to enable safe and effective use of AI, while ensuring appropriate oversight where risk is higher.

2.4.5 Summary

- Most AI use is low-risk and can proceed within guidance
- Some use requires a quick check or advice
- Higher-risk use must follow the formal AI Tool Request Process

If in doubt, ask before you proceed.

2.5 How reliable are generative AIs?

While these AIs are powerful tools that can provide significant benefits, they must be used with caution, and their outputs must always be checked carefully.

Because of their impressive capabilities at having natural conversations with human users, and at confidently solving certain types of problems, such systems may appear to be “intelligent” in a human-like sense. However, it is important to be aware that they lack any common-sense understanding of the

world, intent, motivation, agency, or the abilities of critical and moral judgement we would associate with human intelligence.

You should be aware that, currently, Generative AI systems produce responses based on statistical patterns extracted from huge amounts of data or training they were given, and their developers cannot ensure the responses these systems give are correct. This means that they may provide false information or even fabricate inaccurate responses. The data used for their training may be biased, incomplete, potentially unverified, or not continually refreshed, creating risks of answers that are biased, outdated, inappropriate or lacking context.

2.5.1 AI Hallucinations

AI hallucinations are when artificial intelligence (AI) generates incorrect or misleading information. This can happen when AI models are given tasks that are outside of their training data.

Causes

- Insufficient training data: AI models may not have enough data to provide accurate responses.
- Incorrect assumptions: The model may make assumptions that are not correct.
- Biases: The data used to train the model may be biased.
- Lack of real-world understanding: The model may not understand the real world well enough.

Examples

- AI models have been known to create fake historical records, fabricate legal documents, and spread misinformation about people.
- For example, ChatGPT created a false narrative about a law professor harassing students.

Tips to avoid AI ‘Hallucinations’

- Use data templates to ensure consistent outputs.
- Define boundaries for AI models using filtering tools.
- Test and refine the system.
- Give clear, single-step prompts.

Some providers of Generative AI systems are putting certain safeguards in place to avoid misleading, harmful, abusive, or inappropriate responses are generated, but there is currently little transparency around how this is done, and they certainly provide no explicit guarantees about it.

It is important to understand that the technology landscape around these technologies is rapidly changing, and it is hard to predict whether or when some of these problems may be addressed in future AI systems.

In summary, whilst there are significant benefits, we must also be aware of the negatives. AI output is fallible, and its outputs should be treated as such. There are also significant questions being raised around the ethics of AI and the environmental impact linked to the energy outputs to generate large language models.

2.6 *What are some of the solutions out there and how do I get access?*

The University maintains information on supported AI tools in Appendix 1 / the Supported Tools site. If you wish to use an AI tool that is not currently supported, particularly where University data,

integration, procurement or wider deployment is involved, refer to section 2.4 to determine whether advice or formal review is required.

2.7 How do I get started?

Having read this guidance document so that you have a basic understanding of generative AI, the best way to get started is to explore the University's supported AI tools, including Microsoft Copilot, using the training and resources available through the AI Learning Community.

To start off with, we would recommend exploring the [AI Learning Community Moodle site](#) and the "Starting with AI" section. You can utilise the resources there as a good starting point.

For a more focused approach to boost your productivity, you can use your university LinkedIn Learning access resources such as [this course](#). There are also other specific examples on LinkedIn Learning for you to explore.

2.8 Next Steps

The University has already set up an "AI In Learning and Teaching" consultation group and the AI Learning Community Moodle site (link above) to centralise information on the use of Generative AI.

As also noted, we are exploring how we might obtain licenses for the use of some Generative AI tools at the University.

Be aware that many new AI systems are becoming available, as well as specialist AI systems for imaging, picture generation, media content production, software development and an increased number of other tasks. Each has its own strengths, weaknesses, risks, and benefits.

3. Data- Guidance on the processing of data using Generative Artificial Intelligence

AI systems process information provided through prompts, uploaded content, connected data sources and other interactions. How that information is stored, retained or used varies significantly between AI services and licence types. Staff must therefore use University-supported and approved AI services where University information is involved and must follow the data-protection, security and confidentiality requirements set out in this guidance.

AI systems processing personal data must comply with UK GDPR and the Data Protection Act 2018. The appropriate safeguards depend on both the type of information being processed and the AI service being used.

Personal, confidential, sensitive or restricted University information must not be entered into public, personal or otherwise unapproved AI systems.

Where an approved University enterprise AI service is being used, such as Microsoft Copilot accessed with UWTSD credentials, routine processing of ordinary personal data may be appropriate where:

- there is a legitimate University business purpose
- the personal data is necessary for the task
- only the minimum data required is used
- normal data-protection, confidentiality and access requirements are followed
- AI outputs are appropriately reviewed and are not used as the sole basis for significant decisions about individuals.

Special category or sensitive personal data, unusual or high-risk processing, significant decision-making, or use through systems/integrations that have not already been approved must still be referred through the appropriate University AI review process before proceeding.

Where personal data is not required for the task, staff should remove or anonymise identifiers before providing information to an AI system.

3.1 Compliance with Applicable Laws and Ethical Usage:

All AI usage within the University must adhere to local, national, and international laws and regulations, including data protection, intellectual property, and ethical standards. AI should be used ethically, ensuring fairness, transparency, and accountability in its applications. Discriminatory, harmful, or unethical use of AI is strictly prohibited.

3.2 Data Restrictions and the use of AI

The type of data being processed and the AI system being used must both be considered. Personal, confidential, sensitive, restricted or protected University information must not be entered into public, personal or otherwise unapproved AI systems.

Where an approved University enterprise AI service is being used, such as Microsoft Copilot accessed with UWTSD credentials, routine use of ordinary personal data may be appropriate in accordance with the principles set out in Section 3, provided that only the minimum information necessary for the task is used and normal University data-protection and confidentiality requirements are followed. The following types of information require particular care and may require advice or formal review before being processed using AI:

- special category or other highly sensitive personal data
- safeguarding, disciplinary, grievance, health or other sensitive casework information
- usernames, passwords, authentication credentials or security information
- confidential or restricted University information
- University intellectual property or commercially sensitive information
- copyrighted material where the University does not have appropriate rights or permission for the proposed use
- third-party data where the University does not have appropriate authority to process the information using AI
- information being used to make, support or significantly influence decisions affecting identifiable individuals
- data being processed through new AI tools, integrations, agents or automated workflows that have not already been approved.

Where personal identifiers are not required for the task, they should be removed or anonymised before the information is provided to the AI system.

Where staff are unsure whether the proposed use is appropriate, they should follow the risk-based approach in Section 2.4 and seek advice before proceeding.

4. Use of AI Agents

AI Agents represent an emerging form of Generative Artificial Intelligence designed to act on behalf of a user. These systems can vary significantly in complexity and capability, and it is important to understand the distinction between simpler “chat-style” agents and more advanced “autonomous” agents when considering their use. Staff must take particular care when considering the data and systems to which such agents are granted access.

- **Basic AI Agents** - Basic agents typically function as conversational chatbots connected to approved data sources. Their primary purpose is to retrieve and summarise information or answer user queries based on that data. Examples include chat interfaces integrated into university systems or enterprise tools such as Microsoft Copilot. These agents operate within

defined boundaries and do not take independent action beyond providing information or drafting content.

- **Advanced or Autonomous AI Agents** - In contrast, more complex agents can perform actions on behalf of a user — such as sending emails, creating documents, scheduling meetings, managing files, or integrating with other software systems through APIs or connectors. These agents can chain multiple steps together, access different tools automatically, and complete tasks without continuous human oversight. While these capabilities can enhance efficiency, they also carry significantly higher risks if not configured and governed carefully, particularly around data privacy, access control, and accountability for outcomes.

Regardless of type, all use of AI Agents must comply with the same principles and cautions outlined in this guidance. AI Agents must not be granted access to personal, confidential or restricted University information, systems or services unless that access has been specifically approved through the AI Tool Request Process and appropriate information security and data protection controls are in place.

The implementation of an advanced or autonomous AI Agent should always be treated as a Red use case and must follow the AI Tool Request Process.

5. Use of Generative AI in Research

UWTSD recognises the growing use of Artificial Intelligence (AI) tools and systems in the research process and encourages innovation that advances knowledge and practice. However, the use of AI must be undertaken responsibly and ethically, with full consideration of the implications for research integrity, transparency, and accountability. Research ethics approval does not replace the AI Tool Request Process where the proposed technology/use case meets the red criteria, and vice versa.

Researchers are expected to adhere to the principles within this guidance as well as following principles when using AI technologies in research:

- **Transparency and Disclosure**
Researchers must be transparent about any use of AI tools in their research process. This includes, but is not limited to, the use of AI in literature reviews, data analysis, image or text generation, coding assistance, and writing support. AI use should be clearly acknowledged in research outputs, including publications, reports, and presentations.
- **Accountability**
The researcher remains fully responsible for the integrity, accuracy, and originality of their work. The use of AI does not transfer authorship or accountability. Researchers must ensure that outputs generated or assisted by AI are critically evaluated and verified.
- **Ethical Use and Bias Awareness**
Researchers must be aware of the limitations, potential biases, and ethical risks associated with AI tools, including issues related to data privacy, algorithmic bias, and discriminatory outcomes. These risks should be considered in research design and mitigation strategies should be documented in ethics applications where relevant.
- **Data Protection**
As noted throughout this guidance, personal or sensitive data must not be entered into publicly available AI platforms unless this is explicitly permitted under data protection policies and agreements. Researchers must ensure that any data shared with AI systems complies with relevant privacy, security, and confidentiality regulations.

- **Compliance with Research Ethics in relation to Personal and Confidential Data**
Any research involving the development, use, or study of AI systems must adhere to the UWTSD's Research Ethics and Integrity policy, Trusted International Research and Innovation policy, Research Data Management policy and the university's wider Data Protection and GDPR policies (see section 3). Further, researchers must consider whether the use of AI tools introduces new ethical considerations that warrant formal ethical review, including those related to personal and confidential data.
- **Training and Responsible Use**
Researchers are encouraged to engage in training to understand the capabilities, risks, and ethical dimensions of AI tools. Responsible use involves staying informed of developments and emerging standards in AI ethics and governance.
- **Collaboration**
All researchers engaged in collaborative projects should approach AI tools ethically following a structured, transparent and principled approach that aligns with the core values of research ethics: honesty, integrity, respect, responsibility and fairness. Researchers must ensure transparency regarding use of AI tools at all stages of the research (including at the proposal stage and in relation to any initial discussions with potential collaborators).

Further information can be found below:

- [Research Integrity and Ethics | UWTSD Intranet](#)
- [Trusted International Research and Innovation | UWTSD Intranet](#)
- [Research Data Management | UWTSD Intranet](#)
- [Use of generative artificial intelligence in application preparation and assessment – UKRI](#)
- [Guidelines on the responsible use of generative AI in research developed by the European Research Area Forum - European Commission](#)
- [Understanding artificial intelligence ethics and safety - GOV.UK](#)

6. Legal perspective

The use of Generative AI raises several legal issues that staff should be alert to. These include (but are not limited to):

- **Inputs:** There are potential legal and contractual issues around the extent to which data can be used as inputs for AI systems. Laws protecting the ownership of databases, intellectual property rights and contractual requirements restricting the use of datasets should be considered.
- **Intellectual Property:** Intellectual Property rights must be respected. If AI-generated output infringes the intellectual property of a third party, that party may take legal action against the person or organisation making the output available. AI systems do not necessarily verify whether generated outputs infringe third-party rights. Staff must therefore take appropriate care before reproducing or publishing AI-generated material.
- **Reliability and Equality:** AI products may provide outputs that are inaccurate, incomplete, biased or out of date. Staff remain responsible for checking and validating AI-generated outputs before relying upon them. Staff should also be aware that discriminatory outcomes resulting from the use of AI may contravene protections set out in the Equality Act 2010.

- **Data Protection:** AI systems processing personal data are required to comply with data protection law, including the UK GDPR and Data Protection Act 2018. Personal, sensitive or confidential information must not be entered into public, personal or otherwise unapproved AI systems. Where there is a legitimate requirement to process such information using AI, the system and proposed use must either be permitted under this guidance or otherwise appropriately approved by the University, with the necessary data protection, security and contractual safeguards in place. Please see Section 3 for further guidance.

Appendix 1

The inclusion of a product in this table does not in itself constitute University approval. Staff should refer to the “University status” and “Staff guidance” columns and follow the risk-based approach in Section 2.4. AI services, features and licence arrangements change frequently; the University’s Supported Tools site should be treated as the authoritative source for current supported services.

Solution / Service	Typical use	University status	Data / security position	Staff guidance
Microsoft Copilot / Copilot Chat	General productivity, drafting, summarising, research support, image generation	Supported / approved when accessed with UWTSD credentials	Enterprise Data Protection applies when staff sign in with their work/school account; prompts and responses are covered by Microsoft’s enterprise terms and are not used to train foundation models.	Preferred general-purpose AI service for university work when accessed using UWTSD credentials. Routine use of ordinary personal data may be appropriate where there is a legitimate business need, the information is limited to what is necessary, and normal University data-protection and confidentiality requirements are followed. Personal data should be removed or anonymised where it is not required for the task. Special category/sensitive personal data, significant decision-making, unusual or high-risk processing, new integrations or agentic use remain subject to the risk-based review requirements in Section 2.4.
Microsoft Copilot – integrated Microsoft 365 capabilities / agents	Working with Microsoft 365 content, organisational data, workflow automation and agents	Supported platform, but specific capabilities/use cases may require review	Microsoft states that enterprise controls, permissions, retention, and auditing apply, although controls vary by licence and agent configuration.	Routine low-risk use can proceed. Integrations, agents, automated actions, or sensitive-data use should be assessed under Section 2.4; advanced/autonomous agents are Red.

Solution / Service	Typical use	University status	Data / security position	Staff guidance
Adobe Firefly	Image and creative-content generation	Supported through UWTSD Adobe provision	Existing UWTSD-supported tool. Adobe also provides enterprise governance and controls around Firefly services.	Suitable for approved creative use. Normal copyright, confidentiality, and data requirements still apply.
GitHub Copilot	Software development, code generation and coding assistance	Available/supported for relevant UWTSD users	Current appendix records UWTSD availability. Organisational versions provide centrally managed policies for models, agents, and features.	Appropriate for authorised development use. New integrations, agents, repositories containing sensitive data or wider deployment should follow Section 2.4.
Vevox AI Quiz Creator	Polling, engagement, and AI-assisted quiz creation	Supported through UWTSD licence	Existing UWTSD-supported functionality within Vevox.	Can be used within the existing service and this guidance. Learning & Teaching requirements continue to apply.
LinkedIn AI / LinkedIn Learning AI features	Professional development and learning support	Supported where provided through UWTSD LinkedIn Learning access	Existing appendix identifies the LinkedIn AI Coach as available with UWTSD credentials.	Use within the supported institutional service. Avoid entering information inappropriate for the service.
UWTSD Library AI Research Assistant	Resource discovery and research support	Supported UWTSD service	Existing institutional service.	Can be used within its intended scope and in accordance with Library/research guidance.
ChatGPT – personal/free/Plus accounts	General-purpose chat, drafting, research, coding, and content creation	Not a UWTSD-supported institutional service	Consumer and business offerings have different data terms. OpenAI states that business products such as ChatGPT Business, Enterprise and Edu do not use organisational inputs/outputs for model training by default; this should not be assumed for personal accounts.	Low risk use with public/non-sensitive information may fall within Green/Amber guidance. Do not treat a personal paid account as university approval. Institutional deployment or protected-data use requires review.

Solution / Service	Typical use	University status	Data / security position	Staff guidance
ChatGPT Business / Enterprise / Edu	Managed organisational AI workspace	Supported platform, but specific capabilities/use cases may require review	OpenAI states organisational data is not used to train models by default and provides enterprise security/privacy controls.	Any proposal to procure or deploy organisationally is Red and must follow the AI Tool Request Process.
Google Gemini – consumer service	General-purpose AI, content generation, coding, and research	Not currently supported for institutional use	Consumer and managed Workspace offerings have materially different data protections.	Public/non-sensitive experimentation only where consistent with Section 2.4. Do not use consumer access for protected University information.
Gemini for Google Workspace / Gemini for Education	AI integrated with Google Workspace applications	Not currently identified as a UWTSD-supported service – review required	Google states that Workspace protections apply to Gemini and that organisational content is not used for generative-model training outside the domain without permission.	Any institutional use or integration would require formal review unless separately approved by the University.
Gemini Notebook / NotebookLM	Source-grounded research, document synthesis and study/research assistance	Not currently listed as a UWTSD-supported service	Google now includes Gemini Notebook within its Workspace/Education AI privacy framework; managed Education accounts receive enterprise-grade protections.	Treat personal/public versions separately from managed institutional services. Any University deployment or protected-data use requires assessment.
Claude	General-purpose AI, drafting, analysis, coding, and research	Supported platform, but specific capabilities/use cases may require review	Enterprise offerings exist separately from consumer Claude and provide managed organisational deployment options.	Personal use should be limited to appropriate low-risk information. Organisational adoption or integration requires formal review.
Perplexity	AI-assisted web research and search	Not currently supported for institutional use	Enterprise versions provide different protections from consumer services, including no AI training on Enterprise	Appropriate low-risk use may proceed under Section 2.4. Do not upload protected University

Solution / Service	Typical use	University status	Data / security position	Staff guidance
			data and additional retention/admin controls.	information to personal accounts. Enterprise adoption/connectors require formal review.
Canva AI / Magic Studio	Design, presentations, image/video generation and content creation	Status to be confirmed against UWTSD's Canva provision	Canva provides AI functionality through Magic Studio; its Enterprise service includes administrative, security and AI privacy controls.	If Canva is institutionally provided, confirm which AI capabilities are covered by that agreement. Otherwise treat as an external AI service under Section 2.4.
Grammarly AI	Writing assistance, rewriting, and editing	Not currently identified as UWTSD-supported AI	Current appendix lists consumer functionality but does not establish institutional approval.	Low risk uses only unless institutionally approved. Do not submit confidential or protected information through personal accounts.
Gamma	AI-generated presentations and documents	Not currently supported for institutional use	Current appendix lists the product but does not establish institutional approval.	Public/non-sensitive use may be appropriate; institutional deployment or University information use should follow Section 2.4.
Stability AI / other standalone image generators	Image generation	Not currently supported for institutional use unless separately approved	Existing appendix lists Stability AI but does not identify it as a UWTSD-supported service.	Use only with appropriate information/assets and in accordance with copyright/licensing requirements.
Other AI tools not listed here	Any AI-enabled system, plug-in, application, agent, or service	Not automatically approved	Security, contractual and data-handling arrangements vary significantly between products and licence types.	Apply Section 2.4. Low-risk use may proceed where appropriate; unfamiliar tools should be treated as Amber, while procurement, deployment, integration, sensitive data, or higher-risk decision use is Red.