THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Operational

AI Legal and Regulatory Guidance

Table of Contents

What this guidance is for

This guidance has been produced for staff and students who want to use AI (mainly generative, but also predictive) so that they are aware of the legal and regulatory issues that relate to AI. The intention is to provide you with the guidelines you must operate under so you do not breach any laws while using AI. As such we cover:

- competition law and confidentiality
- copyright
- cybersecurity
- data protection
- equality act, including bias and discrimination

We also highlight upcoming or proposed laws at the end of this document.

General points for using AI

1. What is the AI for?

Think about the purpose of using AI for the task you want to use it for. While it is fine to play about with the tools as you are learning to use them, you can avoid most of the legal and regulatory pitfalls relating to AI by understanding what it is you want to do. Like all tools, AI is most helpful when you know what you are using it for.

2. How will the use of AI make things better?

AI tools are meant to simplify your work, so consider what improvements they'll bring before you start using them. Avoid using a tool just because it's available. Use it because it will make a task like analysis quicker or help you start a writing task by providing prompts or a draft to work on. When using AI for your intended task, it's crucial to have a clear purpose in mind. Experimentation is encouraged, but always be mindful of the legal and regulatory implications associated with AI, particularly Generative AI use.

What is AI - definitions

AI - For the purpose of this guidance, when we mention AI we mean 'A digital system that exhibits human-like cognitive abilities including but not limited to learning, problem solving and content generation'. AI comes in two main forms, generative and predictive.

Generative AI – creates synthetic content that mimics human creativity. So can be used to create texts, images, sound from content already fed into it. E.g. policy drafts, images to include in texts.

Predictive AI - predicts future trends and behaviours based on historic data. E.g. characteristics of successful applicants, what food sells better summer versus winter.

Public AI – an AI system that anyone can use e.g. the free version of ChatGPT.

External AI – an AI system not provided by the School. These can be Public AI or may be paid versions of a tool that mean that you can ensure your data is not reused by the system.

What AI tool does the School provide

The School provides MS Copilot. This stays within the School's M365 tenancy so is safer to use as long as you have the correct access controls set on your information. You can use Copilot for creating summaries of copyrighted work which you would not be allowed to feed into a commercial AI that would use the content for training.

What not to do

- Don't put personal data in an AI tool that is external to LSE. If it will swallow the personal data for further processing that LSE cannot control, you can't use the AI tool.
- Don't upload in-copyright content (for example , images, photographs, student work, journal articles licensed from publishers by LSE library) where you do not have the copyright holder's permission and where the AI tool is known to use inputs as training data.
- Don't put confidential or commercially sensitive data in an AI tool that is external to LSE. Aside from breaching confidentiality simply by feeding it to the AI, it is also likely that the data can be regurgitated, that is disclosed to an indefinite number of third parties outside your or LSE's control.
- Don't look for LSE's competitors' data that can be regurgitated either.
- Consider access rights when linking your OneDrive or any personal cloud storage to an AI tool. You may not want to give it access to everything. If you do, potentially a copy of your personal ID could be fed to the AI tool.
- Don't ask an AI tool to do something malicious or illegal.

Think about

- As AI gets better, it will appear to be 'thinking' more. However, it won't be actually thinking, it is just supporting human thinking.

- How you incorporate checks into processing done by AI. Use your knowledge and common sense on the results it provides you.

Has the AI tool got the intellectual property rights to be providing you with the outputs it has given you. Check if you are not certain.

Do

Familiarise yourself with the terms and conditions of the Generative AI tool, including data retention, reuse policies, and any licensing agreements required.

Show its working with a direct quote, to make it easier to verify (verification is always needed, but showing its working makes the process a lot less painful).

Conduct an Equality Impact Assessment if there is a chance of data leading to bias or discrimination.

Consider who will be a human reviewer of any processing if required by law (Article 22 of the UK GDPR).

Consider how you will explain what the AI tool was meant to be doing.

Competition and confidentiality

As a university, LSE is subject to competition law. We also have to keep our own commercially confidential data secure as well as the commercially confidential data of our suppliers or other stakeholders.

Competition law requirements

That the School does not share data or discuss any of the following with potential competitors:

- Future pricing intentions e.g. course fees
- Student numbers

The more detailed the data, the more likely it is to breach competition law.

Confidentiality requirements

Information is confidential in nature if:

- The information has the necessary quality of confidence, that is, not in the public domain, not well known to most people.
- The information was imparted with an expectation of confidence in a contract or in a particular situation e.g. to a counsellor.
- By disclosing the information, the discloser of the information suffers a detriment e.g. a competitor finds out the prices of a company.

There may be situations where, with some exceptions, you are expected, or obliged not to disclose confidential information, for example when accessing datasets that have been licenced to the School under a confidentiality clause within a wider contract or a stand-alone confidentiality agreement or non-disclosure agreement (NDA). Or you may have obtained information in confidence, and it cannot be disclosed without the discloser's consent or misused to prejudice the discloser. For example, if you come across confidential information as part of a collaborative project with an external stakeholder, you are expected not to disclose it.
A breach of confidentiality may cause financial losses, reputational damage, can expose the School to serious liability and you may incur disciplinary sanctions.
Whatever your role is, you should be careful in handling information that you are aware or suspect may be confidential, especially when it come to the use of AI tools.

Competition and confidentiality AI issues

Before feeding any information in a public AI system, please consider that:

- communication of confidential information to a public AI system is already a breach of confidentiality, because with some limited exceptions you are not supposed to disclose it to anyone, including the AI system.
- Any information fed into a public AI system may be re-used and disclosed to an indefinite number of third parties by the AI system.
- The School expects that you take responsibility of your use of AI and make sure that it is done in the respect of third parties' rights including their right to confidentiality.
- The School cannot use public AI systems for processing tenders as this could make the commercially sensitive pricing data available to third parties including their competitors.
- Any information which could potentially be considered breaching competition law should also not be put in a public AI system as this could be regurgitated.
- We should not try to get a competitor's data out of an AI system by trying to get it to regurgitate that data.

Copyright and intellectual property

Copyright

The Copyright, Designs and Patents Act 1988 (CDPA) is the key piece of legislation underpinning copyright law in the UK. Copyright protects original creative works, granting authors control over how their work is copied and shared. The CDPA is a complex piece of legislation, but in brief works covered by copyright include books, music, paintings, photographs and films, broadcast, databases, logos and other branding and newspaper articles, just to mention a few examples. In UK, the owner of copyright in a work has certain rights, and (with some exceptions) their permission is needed in relation to the certain acts including:

- Reproduction – copying the work, including photocopying, scanning, downloading;
- Distribution – issuing copies of the work to the public in print or online (this also covers rental and lending of the work);
- Public performance – includes performing, transmitting or broadcasting a work to the public;
- Display – showing a work or a portion of a work to others.
- Adaptation – adapting the work.
- Licensing the work to third parties.

As well as these economic rights, the copyright owner also possesses moral rights, which means that they have the right to be identified as the owner and to object to derogatory treatment of their work. Copyright infringement occurs when a person, without the copyright owner's permission, performs any of the acts mentioned above.

There are some specific permitted acts where copyrighted works can be used without infringement. These include for example "fair dealing" with certain types of copyright work for the purposes of research and private study; criticism or review; reporting current events; quotation; or parody, caricature, pastiche. Use of works in educational settings, such as teaching and examination purposes, is allowed under specific conditions. This includes the use of extracts in academic materials.

Copyright and AI

The CDPA was drafted before the possibilities and challenges of GenAI were known. Law, and the governments that make it, are lagging behind developments in this area. There is, therefore, considerable uncertainty around who is the owner of the copyright in an AI generated work and what actions should, or should not, be considered copyright

infringement when it comes to the use of AI systems. A delicate balance is needed to promote innovation while safeguarding the intellectual property rights of creators. Copyright is territorial, that is, the law is different depending on the country in which you live, and this is a further complicating factor. Actions that may be permissible under US law, for example, may be seen as problematic within the UK.

There are currently a number of legal cases in progress challenging the legality of the use of copyright works to train GenAI (LLMs and images) without copyright holder permission. New legislation is also coming in to force, for example the EU's Artificial Intelligence Act. It is, therefore, likely that there will be some clarification in this area in the medium term.

Copyright AI Issues

1. Data Input: Inputting copyrighted content owned by someone else into an AI tool could potentially infringe their copyright, depending on how much of such content is input, the applicability of any legal/contractual exception and how the content is transformed or utilised by the AI system. It's important to ensure that you have the rights to use the copyrighted material, and that you do not share confidential or protected materials while feeding data to the AI tool. Additional precautions include avoiding the use of third-party IP in prompts to minimise infringement outputs, seeking tools that use properly licensed or public domain training data or have technical safeguards against using protected data, and vetting datasets when training AI to consider IP ownership and licence coverage.
2. Text and Data Mining: the TDM exception (Section 29A CPDA) permits anyone who has lawful access to in copyright material (e.g. through an institutional subscription) to make copies of it in order to carry out computational analysis for the purpose of non-commercial research. These copies must not be shared with any unauthorised users. Inputting licensed content from library subscriptions into GenAI tools can be interpreted as permissible computational analysis. However, if the tool retains copies of the inputted material this is likely to be interpreted as infringing copyright because it would be accessible to others not covered by the exception. Please note that the TDM exception only covers TDM carried out for research for a non-commercial purpose. Please be aware that the interpretation and application of the TDM exception may be tricky at times, so be careful if you wish to resort to it, and if in doubt seek advice. When using GenAI with library licensed content, ensure the tool does not store inputs or use them to train data. If carrying out TDM on material licensed under Creative Commons check the terms of the licence to ensure compliance[1].
3. Data Output: The ownership of work created by AI tools can vary based on the terms of service provided by the AI tool's provider and the jurisdiction's

[1] This is based on text from: Guidance on resisting restrictive AI clauses in licences - Artificial intelligence (jiscinvolve.org)

copyright laws. Always review the terms and conditions of generative AI tools to understand who owns the copyright. Iff the output reproduces a substantial part of a third-party copyright work because the system was trained on that work, then potentially there may be an infringement. AI tools should use legally obtained data for training to avoid copyright infringement and the creation of unauthorised derivative works. Where possible, check for potential copyright infringements before using outputs.

Cybersecurity

Secure AI

MS Copilot is configured to only make use of data you have access to via your M365 account. It does not remember queries, and will not reuse your data or otherwise ingest it for further training and potential regurgitation by other customers. On this basis, MS Copilot supplied via LSE is the safest AI tool you can use. There may be business reasons why it is better to use another tool, however. If another tool is required, Cybersecurity should be contacted and a Cloud Assurance Questionnaire completed before the tool can be used.

Cybersecurity AI rules

1. Any information you input into an AI prompt, or ask an AI tool to analyse, may be stored by the AI provider and used to help further train its products and models.
    a. This also means that any data you supply may surface in responses made to other people's queries. If this is personal data, this constitutes a data breach.
    b. Therefore, *do not* ingest any personal data into AI tools.
    c. This includes your password(s) and usernames.
2. If uploading files to be analysed by an AI tools, ensure they do not contain Personally Identifiable Information.
    a. Even if the data you are extracting from the files is not personal, if the files also contain personal data, that data is available to be consumed by ChatGPT.
    b. Ensure any file uploaded is appropriately edited so it contains the *minimum viable data* necessary to achieve your objective.
3. If linking e.g. Google Drive or OneDrive to an AI tool, ensure it only has access to files that do not contain either personal data or other data that should be restricted only to LSE (e.g. corporate financial data).
    a. Do not link your whole LSE OneDrive to an AI tool.
    b. If you cannot guarantee that you are only linking individual files to an AI tool, rather than your whole drive, or you are otherwise not sure if this stipulation can be met, *do not proceed with linking your file stores*.
4. Don't share other sensitive or copyrighted data.
    a. If you need to use such information, use MS Copilot, which has built in security against such data being reused or ingested into the model.
    b. Remember that you're always accountable for any decisions you make, so be very wary of making decisions solely based on AI outputs.
    c. Any automated decisions that have real-world impacts on humans must allow for a human review.
5. Do not trust any information supplied by AI tools without undertaking independent verification.

    a. AI tools are known to hallucinate, namely supplying information that has no basis in reality, or else reproducing information that is out of date or is misinformation.
6. Never ask an AI to perform tasks that are malicious or that may compromise other people or data that is not yours. This at a minimum would constitute a breach of the Computer Misuse Act 1990, the Terms of Use of Jisc's network, our M365 tenancy agreement and the standard terms of most AI tool providers.

Data Protection

Personal data

Personal data is defined in the UK GDPR as ‘any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person’.

Personal data at LSE includes assessments, audio and video recordings, transcripts of audio and video recordings as well as the more obvious staff, student and research data.

The natural person referred to above is also called the data subject i.e. the individual who is the subject that the personal data relates to.

Data Protection principles and AI

1. the data is necessary for the purpose (minimisation principle);
   As with all personal data processing, only process the personal data you need to in an AI tool.
2. the use of the data for that purpose is lawful (lawfulness principle);
   Keep personal data processing in lawful AI tools like Copilot. Do not share personal data with external AI tools.
3. the purpose has been explained to the people the data relates to (transparency principle);
   This is particularly important where use of the AI will have a legal effect on someone e.g. marking summative assessment, processing an application.
4. the purpose falls within people’s reasonable expectations or it can be explained why any unexpected processing is justified (fairness principle);
   Consider if you would be happy for your data to be used in the way proposed or if other people are likely to be happy with it.
5. whether the stated purpose aligns with the scope of the processing activity and the organisation’s ability to determine that scope.
   Don’t just use AI because you can, but because it helps processing the data.

The regulator for data protection, the Information Commissioner’s Office has an AI toolkit that can be used when developing or using AI.

Data Protection AI issues

1. **Security:** we are required to keep personal data secure. As most commercially available AI services will keep any data given to them for processing, they are not compliant with the 6th Data Protection principle.
2. **Transfer outside the UK:** we are required to only transfer personal data outside the UK where we have applied one of the derogations in Article 49 of the UK GDPR e.g. contract, consent from the individual. As the most popular AI services are outside the UK and generally unwilling to enter into contracts that will keep personal data secure, we cannot be compliant with the UK GDPR while using them.
3. **Article 22 of the UK GDPR:** data subjects 'have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'. Where we are using AI in a way that produces legal effects, data subjects need to know about this and have the right to request human review e.g. if an AI is used for marking, students need to be told their data will be processed this way and have the right to appeal for a human review.

The Equality Act, bias, and discrimination

What is the Equality Act?

The Equality Act 2010 prohibits both direct and indirect discrimination on the grounds of protected characteristics. These are sex, race, age, religion, disability, sexual orientation, pregnancy/maternity, gender reassignment and marriage/civil partnership.

Direct discrimination occurs when a person receives less favourable treatment directly because of a protected characteristic. Indirect discrimination can occur when everyone is treated the same, but people with a protected characteristic are put at a disadvantage.

The Equality Act also places a duty on employers to ensure that reasonable adjustments are made to reduce or remove disadvantages that may be faced by people with disabilities.

Bias and discrimination risks with AI

Generative AI tools can produce believable content with human-like results. However, the information is based on large volumes of data, some of which can be inaccurate, biased, or discriminatory. Human judgement and filtering for what may be appropriate and reliable is not applied.

In addition, the use of AI tools to process decisions and generate outputs may lead to discrimination based on protected characteristics. Without appropriate due diligence and human accountability, the use of AI can lead to breaches in equality legislation.

In using AI, there should be appropriate scrutiny of:

a) The risk of profiling. Profiling involves categorising people and predicting their behaviour based on their characteristics. This present discrimination risks.
b) Automated decision-making. This is where decisions are made by automated means without human involvement. AI tools can produce unreliable information and where processes are automated, they may not adequately account for exceptions, mitigation or the need for reasonable adjustments. In using AI, you should consider the need for the appropriate and timely use of professional judgement.

Under UK GDPR solely automated decision-making, including profiling, that has a legal or similarly significant effect, is generally prohibited. However, there are exceptions to this. In these cases, safeguards must be put in place.

Bias and discrimination AI issues

a) **Equality Impact assessments (EIAs).** This assessment can help to identify and evidence the likely impact of AI tools on different groups of individuals and where

possible, advance equality, diversity and inclusion. Guidance for carrying at an **EIA** can be found here at LSE.

b) **Issues of transparency:** Consider whether there is transparent enough use of AI tools. Where processes and decisions affect people and their personal data, they should be made aware of how the AI is being used and how their data is being processed. Consider how people will be signposted to this information and how you will gain any necessary consent prior to use.

c) **Explainability:** Where the output of an AI tool has influenced decision making or where an AI automated process is used, there should be someone appropriately trained and/ or informed to provide an explanation for how the AI tool has been used. Staff will not be required to have a deeply technical understanding of the AI tool, but may be able to explain the principles, parameters and / or data that had been applied in the process.

d) **Human decision making:** Human involvement will not necessarily be equal to human decision making. There will a difference between a cursory 'rubber stamping' of outputs and the reviewing of data and applying human professional judgment. Where the use of AI presents a high risk to individuals- for example, in employment decisions, human decision making should always be used appropriately.

e) **Accountability:** AI can be used to generate a range of information and resources. However, given the risks outlined in this guidance, it will be important that necessary steps are taken to review the outputs of any AI tool and ensure that it is accurate, appropriate and has not infringed upon any individual rights or copyright. There should be appropriate accountability for ensuring that these necessary steps have been taken.

f) **Auditing and Monitoring**: Consider how the use and outputs of AI will be monitored and reviewed. This could be built into existing review processes.

g) **Staff training and guidance**: The School encourages staff to have a basic understanding of AI, how it can be used and be familiar with the potential risks of using it. In addition, where AI is used within teams and / or had been embedded into working practices, there should be appropriate training and technical knowledge for the staff involved.

Legislation affecting AI use

Acts and Bills affecting UK HEIs and Organisations related to competition and confidentiality, copyright, cybersecurity, data protection, employment and working practices- as at June 2024.

This section will be updated as required.

EU AI Act

Will apply to – personal data, employment and working practices, competition

The aim of the Act is to be the world's first comprehensive legal framework on AI worldwide. The levels of regulation in this Act are applicable to UK based companies who operate globally and the main approach of the Act is based on defining risks, defining key players, and outlining penalties for employers/organisations. This Act is intended to complement EU GDPR rules which are mirrored in UK GDPR.

The Act has aligned its definition with the OECD's definition of AI, that "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 Act makes it clear the key distinguishing factor is the AI system's capability to infer something; basic and very commonly used automation tools are therefore out of scope.

The AI Act classifies AI systems into four **categories** of risk: unacceptable, high, limited, and minimal. The rules that apply to the system will turn on that classification:

a) Unacceptable risk: systems that contravene the EU's values and fundamental rights and their use is prohibited.
b) High risk: these pose a significant threat to the health, safety, or fundamental rights of individuals or groups and are subject to strict requirements. This one is most relevant to employment and student recruitment, in particular in recruitment practices.
c) Limited risk: these pose a moderate threat to the rights or interests of individuals or groups and are subject to transparency obligations.
d) Minimal risk: these pose a negligible or no threat and are not subject to mandatory requirements.

The core ideology is to protect humans from risk to health, safety and fundamental rights of natural persons.

The European Parliament agreed the EU AI Act in March 2024 and the following **principles** should be considered in relation to the use of AI and working practices:

a) Assessment and mitigation of risk
b) Fairness, bias and discrimination
c) Transparency and explainability
d) Human decision making
e) Accountability and redress

UK AI Regulation Bill

Would have applied to: any potential use of AI in the UK.

A private member's bill that will not move forward due to the election.However the principles in this Bill, include that the UK House of Lords AI Authority that has been proposed, could be taken up in similar legislation in the next Parliament. This bill proposed:

1) safety, security and robustness;
2) appropriate transparency and explainability;
3) fairness;
4) accountability and governance; and
5) contestability and redress.

TUC 2021 Manifesto on AI

Will apply to: employment and working practices

This is currently being developed with the aim of safeguarding workers. It's called Dignity at work and the AI Revolution.

Review schedule

Review interval	Next review due by	Next review start
1 years	31/10/25	01/10/25

Version history

Version	Date	Approved by	Notes
2	24/10/2024	AI Working Group	

Links

Reference	Link
N/A	N/A

Contacts

Position	Name	Email	Notes
Data Protection Officer	Rachael Maguire	glpd.info.rights@lse.ac.uk	
Director of Cyber Security & Risk Management	Jethro Perkins	Dts.cybersecurity.and.risk@lse.ac.uk	
Copyright Officer	Wendy Lynwood	library.copyright@lse.ac.uk	
Senior Legal Counsel	Mariachiara Valsecchi	Secdiv.Contracts@lse.ac.uk	
HR Partners	Solmaz Kolahi / Beno Azebiah	Hr.Partners@lse.ac.uk	

Communications and Training

Will this document be publicised through Internal Communications?	~~Yes~~/ No
Will training needs arise from this policy	Yes/ ~~No~~
If Yes, please give details TBC	