

Policy Name:	<i>E-Safety Policy and Procedure</i>
Policy Ref:	POL/ES/CLS/001
Who it applies to:	Learners, Employees and ASC
Date of issue:	Version 0.6
Date last revised:	October 2024
Policy Type:	CLS
Policy Owner:	Dean/Deputy Dean of CLS
Approved by:	SMT
Last Review Date:	August 2026
Review Due Date:	August 2027
Equality Impact Assessment Screened	Yes
Contractual Terms and Conditions, which will be changed following legal requirements.	No

E-Safety Policy and Procedure

E-Safety Policy and Procedure

Contents

1. Introduction.....	2
2. Purpose and Scope.....	2
3. Roles and Responsibilities	3
4. E-Safety Incidents	4
5. Reporting Incidents	4
6. Monitoring and Review of this Policy	4
7. Useful E-Safety Resources	5
8. Associated Policies	5
Appendix 1: E-Safety Guidelines	6
Appendix 2: E-Safety Incident Report Form	11
Appendix 3: Social Media Accounts - Right to Object to AI Data Scraping	12

1. Introduction

The Internet and other Digital and Information Technologies are powerful Tools, which can stimulate discussion, promote creativity and promote effective learning. We encourage the use of technologies, in order to enhance skills, promote achievement and enable lifelong learning.

These technologies can also put individuals at risk. Some dangers that may be faced are:

- Data Protection and IT Security infringements, such as data breaches, unauthorised access to, loss of or sharing of Personal Data.
- Risk of being groomed or radicalised.
- Access to illegal, harmful or inappropriate website images, games or content.
- Cyber-Bullying.
- Plagiarism, Copyright and Intellectual Property Infringements.
- AI Hallucinations and AI Bias are issues, when using AI Platforms.

2. Purpose and Scope

This Policy addresses the risk of (mis)use of technology, which affects the welfare of others or where the culture or reputation of CILEX Law School is put at risk. The use of technology, includes, but it is not limited to:

- Email.
- the Internet.
- Software and Cloud Based Storage or Software.
- the VLE (CLS Hub Aptem), associated Forums and Webinar Rooms (MS Teams).
- Social Networking Sites and Social Mobile Apps (including owners of Social Media Companies, such as Meta (Facebook and Instagram) and LinkedIn, which are carrying out data scraping of all Social Media Account's content (including Posts, Photos and Tags) to collate and contribute to publicly accessible AI Platform's content to be searched or queried by AI Prompts). (Note: You can only opt out of the AI Data Scraping of your Social Media Account by completing the Right to Object Form online for each Social Media Account). For further information, please see Appendix 3.
- Mobile Phones.
- MS Teams.
- Use of AI Platforms (either publicly or privately accessible AI Platforms) and AI Devices (such as Humane AI Pin or AI Friend).

This Policy applies to Learner's online behaviour that is linked to the CILEX Law School in any way. Staff usage of technology is covered by a range of associated Staff Policies.

CILEX Law School Learners do not use any equipment, which is the property of the CILEX Law School. CILEX Law School Learners use, either their own devices or devices provided by their Employer. When using devices and systems, which are provided by their Employer, they should adhere to the Employer's IT Policies and Procedures.

CILEX Law School cannot eliminate the risks associated with the use of technology, but it will address these risks through regular training and our E-Safety Guidelines (Appendix 1).

AI Governance and Use:

When using any AI Platform, you do not input any Personal Data (including Special Categories of Personal Data), any photos or video featuring Data Subjects (particularly, without the Consent of the Data Subject), confidential business information, Company Logo (which is Copyright) or any other material

that is subject to Copyright or Intellectual Property Rights. You must check sources of information are accurate and active, if you are using an AI Platform to search for information, please be aware that any search results are still subject to the Copyright, Plagiarism issues and Intellectual Property Rights, as with any website usage and that any quotes or sources must be accurately acknowledged and referenced in any assignments. Therefore, you need to be mindful of AI Bias and AI Hallucinations.

CLS Students are only permitted to use AI Platforms for their Law and Practice Units Assignments, but it is not permitted to be used for any other assignments or any online exams (including not using any AI Devices, such as Humane AI Pin or AI Friend).

Please see the CLS Privacy Statement and CLS Disciplinary and Malpractice Policy and Procedure for further information.

3. Roles and Responsibilities

3.1 Dean of CILEX Law School

The Dean of CILEX Law School will be responsible for overseeing the E-Safety of the CILEX Law School Learners. Day-to-day responsibility for implementing and monitoring E-Safety is delegated to the Head of Apprenticeships.

3.2 Head of Apprenticeships

The Head of Apprenticeships will be responsible for the implementation and monitoring of this Policy. The Head of Apprenticeships will ensure that both Staff and Students have access to the appropriate training, in relation to E-Safety.

3.3 Designated Safeguarding Officer (DSO)

3.3.1 The DSO will be trained in E-Safety particularly on core sections of the Online Safety Act 2023 and the Crime and Policing Act 2026, and they will be aware of potential issues, which may arise from:

- Data Protection and IT Security infringements, such as data breaches, unauthorised access to, loss of or sharing of Personal Data.
- Risk of being groomed or radicalised.
- Access to illegal, harmful or inappropriate website images, games or content.
- Cyber-Bullying.
- Plagiarism, Copyright and Intellectual Property Infringements.
- AI Hallucinations and AI Bias are issues, when using AI Platforms.
- Cybercrime
- Inappropriate images created using AI or self-generated by the child

3.3.2 The DSO will deliver Staff Development and Training, record and report incidents or any developments and they will liaise with the Local Authority and External Agencies, where appropriate.

3.3.3 The DSO will provide pastoral and practical support for Students dealing with issues that are related to E-Safety.

3.4 Staff

Staff are responsible for ensuring that:

- They have an up-to-date awareness of the E-Safety Policy and Procedure, as well as the CILEX Acceptable Use Procedure and other CILEX IT Security related Policies and Procedures.
- E-Safety is embedded in Teaching, Learning and Assessment, where appropriate.
- Learners have an understanding of research skills and how to avoid plagiarism. They should report any suspected misuse or problems through the appropriate channels

3.5 Learners

Learners are responsible for ensuring that:

- They report suspected abuse, misuse or access to inappropriate materials.
- They comply with the Student Code of Conduct and CILEX Code of Conduct.
- They keep their log in details and passwords secure, confidential and that they do not share them with anyone else.

4. E-Safety Incidents

An E-Safety incident is considered to have occurred, when a Learner or Member of Staff is the victim of an activity utilising technology to endanger the personal safety, mental or financial wellbeing of another individual or where the culture or reputation of the CILEX Law School is put at risk.

E-Safety Incidents may be categorised under three core areas: Safeguarding, Discipline and Cybersecurity. These are not mutually exclusive and concerns may fall under one or all areas, in certain circumstances.

Every E-Safety Incident will be assessed, in relation to Safeguarding, Discipline and Cybersecurity Risk. Typically, however, E-Safety concerns will be dealt with in the following way:

- Safeguarding Issues will be managed by the DSO, in accordance with the Child Protection and Safeguarding Policy.
- Learner Discipline Issues will be dealt with, in accordance with the Disciplinary and Malpractice Policy and Procedure.
- Staff Discipline Issues will be dealt with under the relevant Staff HR Policy.
- Cybersecurity Issues will be dealt with by the Information Technology Team and/or Digital Learning Lead depending on the nature of the issue.

5. Reporting Incidents

Incidents should be reported to the Designated Safeguarding Officer (DSO) using the Incident Report Form (Appendix 2).

The incident will be logged on the E-Safety Report and Actions Log and reviewed by the DSO and Head of Apprenticeships Quality and Compliance.

CILEX Law School will deal with E-Safety Incidents in the same way, as Safeguarding and Prevent Issues and when appropriate, will refer the issues to:

- MASH (Multi-Agency Support Hub).
- Police.
- Prevent

6. Monitoring and Review of this Policy

The implementation of this Policy will be monitored by the Head of Apprenticeships. E-Safety Incidents will be an integral part of the continuous Safeguarding Development, Monitoring and Review and they will be included in the monthly report to the Apprenticeship and Safeguarding Committee.

The Policy will be reviewed annually or more frequently, if there have been any significant new

technology developments, E-Safety threats or incidents.

7. Useful E-Safety Resources

- SWGfL: [E Safety Facts - Staying Safe Online | SWGfL](#)
- SWGfL: <https://swgfl.org.uk/products-services/online-safety/resources/>
- Cyber Aware: [Cyber Aware - NCSC.GOV.UK](#)
- Safer Internet Day: [Home - Safer Internet Day](#)
- Get Safe Online <http://www.getsafeonline.org>
- Cyberbullying.org - <http://www.cyberbullying.org/>
- Internet Watch Foundation: <https://www.iwf.org.uk/>
- Think You Know: [Thinkuknow - home](#)
- Information Commissioner's Office (ICO – UK's Data Protection Supervisory Authority): <https://ico.org.uk/>
- National Cyber Security Centre (NCSC): [National Cyber Security Centre - NCSC.GOV.UK](#)
- AI Safety Institute (UK): [The AI Safety Institute \(AISi\)](#)
- DRCF (The Digital Regulation Cooperation Forum – UK – Comprises of the Regulators ICO, CMA, Ofcom and FCA): [Home | DRCE](#)
- European AI Office: [European AI Office | Shaping Europe's digital future \(europa.eu\)](#)
- Online Safety Act 2023: [Online Safety Act - GOV.UK](#)
- House of Commons, Social media, misinformation and harmful algorithms: [Social media, misinformation and harmful algorithms](#)
- Crime and Policing Act 2026 - [Crime and Policing Act 2026](#)

8. Associated Policies

The following Policies are associated with this Policy:

- Safeguarding and Prevent Handbook
- Equality, Diversity, Inclusion and Accessibility Policy
- Accessibility Procedure
- Student Code of Conduct
- Learner Disciplinary Procedure
- Teaching, Learning and Assessment Policy
- Staff Grievance Procedure
- Staff Disciplinary Procedure
- CLS Disciplinary and Malpractice Policy and Procedure
- CLS Privacy Statement
- CILEX Information Security Policy
- CILEX Information Technology (IT) Policy
- CILEX Data Protection Policy and Procedure and CILEX Privacy Statement
- Acceptable Use Procedure
- Information Security Procedure
- IT Security Incident Management Procedure

Appendix 1: E-Safety Guidelines

1. The forums on our Virtual Learning Environment are secure and they are only accessible to registered Students. They are monitored by Staff, although this cannot be done on a synchronous basis. We, therefore, expect Students to maintain the highest of standards of behaviour, when using our online forums.
2. Remember that the CILEX Law School's Code of Practice for Students applies to behaviour online, as well as face-to-face.
3. Unacceptable Behaviour will be dealt with, in accordance with our Disciplinary Policy. Sanctions can include the termination of your course. If your course is being sponsored by your Employer, we reserve the right to notify your Employer that you have been subject to Disciplinary Action.
4. Unacceptable Behaviour online can take many forms. This includes, but is not limited to:
 - Cyber-Bullying.
 - Posting or re-posting abuse.
 - Posting or re-posting offensive or defamatory images or using offensive or defamatory language (or images or language likely to cause offence).
 - Posting or re-posting discriminatory material.
 - Posting or re-posting anything that may bring CILEX Law School into disrepute or threaten the safety of staff (including former staff) and students or anyone connected with the CILEX Law School.
 - Harassment.
 - Hate speech (i.e., abusive or threatening speech or writing that expresses prejudice against a particular group, especially on the basis of race, religion or sexual orientation).
 - Collusion or Plagiarism.
 - Intentionally sharing sources which have been identified as including misinformation and disinformation.

The Online Safety Act 2023 introduced new rules for internet companies to ensure users are protected from harm that can place on their platforms, including tackling harms to individuals from illegal material online, and to better protect children. The OSA made Ofcom the UK regulator for online safety.

The OSA created a new duty for online platforms and a similar duty for search engines to assess the risks and mitigate the harms stemming from two types of material: illegal content, including fraud, terrorism and other offences; and content that is harmful to children.

5. Students are not required to engage on social media. Do not feel obliged to engage or connect with any Student on social media. Do not pressurise other Students to engage with you on social media.
6. Remember that the comments that you post on social media can impact on your professional reputation: consider your cyber footprint. Prospective Employers may check your social media profile/s. The posts you 'like' and the organisations that you follow may be used by others to form a judgement about you.

In addition, social media platforms (including LinkedIn and Meta, which own Facebook and Instagram) are allowing data scraping practices for the purposes of collating your information from your social media accounts that includes posts, photos and tags (regardless of, if you post to friends/contacts only) and this information is being entered into publicly accessible AI Platforms, which can be searched by anyone worldwide that uses the AI Platform (this means that anything other than currently your

messages becomes public information on a worldwide basis and it can be accessed by an AI Prompt search). So, it is particularly important that you not to enter any comments that constitute a breach of the Equality Act 2010, anything that would constitute defamation of character against another individual, any comments about an Employer or Other Member of Staff (which could mean that you are subject to Disciplinary Action or a Legal Claim) or any breach of an NDA or Confidentiality Agreement that you have signed i.e. with an Employer or you should have not released any business confidential information. You can complete a Right to Object Form on each social media account (Specifying your reasons under UK Data Protection Legislation, such as they do not have the "Consent of the Data Subject", i.e., your permission to data scrape your account for the purposes to collating information for an AI Platform, etc.), delete historical posts, photos or tags or close down or restrict what you post on certain social media accounts. It is also the case that you should not post photos of other people (Data Subjects) without their written consent, as is the case with any online uploaded photo and in particular, due to the current practice of AI Data Scraping the Internet and Social Media Platforms. For further information, on your Right to Object on Social Media accounts, please see Appendix 3.

7. Before making a posting, always think about the impact that your post may have on others. Treat others with respect.

Misinformation vs disinformation:

There is access to vast amounts of information due to social media which spreads faster than ever before, however this comes with the challenge of tackling fake news. Misleading and harmful content on social media can lead to unrest within communities.

"Harmful content" is defined in the Online Safety Act 2023 as physical or psychological harm. Content that is harmful includes harm arising from the nature of the content and the fact or manners of its dissemination.

"Misinformation" can be defined as verifiably false information that is shared without an intent to mislead and "disinformation" as verifiable false information that is shared with an intent to deceive.

"Platforms and companies" is the term used to describe an online service that hosts contents. The term "company" is used to describe the business that owns and runs that platform.

An "algorithm" is set of instructions a computer follows to performs tasks or solve problems. A recommendation algorithm is a type of algorithm designed to suggest data or content based on patterns in user behaviour or preferences. A social media recommendation algorithm selects and promotes content or accounts that is predicts will engage users, shaping individual feeds and influencing what users see, usually aiming to increase engagement and time spent on the platform.

Social media algorithms can contribute in promoting misinformation and harmful content. The principle of maximising engagement for profit means that algorithms can amplify content regardless of accuracy or potential for harm. False and harmful content is often designed to be engaging, so may be promoted more than other types of content. Examples include mis/disinformation, violence, extremism, prejudiced views, suicide and self-harm content.

8. It is important that students can participate in free and open academic debates on our forums (subject to our Code of Conduct). Please do not share comments from a CILEX Law School Forum publicly.

9. Please do not share Personal Data (including Special Categories of Personal Data), in relation to a fellow student without their written Consent of the Data Subject (Personal Data) and their explicit consent (Special Categories of Personal Data). Do not name fellow students or staff on public forums or social media in a critical or derogatory way. This is not intended to prevent you from using social media to talk about CILEX Law School or to express critical views appropriately. However, you should not

publicly criticise individuals and you should use the appropriate Complaints Procedure instead.

10. Please do not share any CILEX Law School materials or recordings of webinars on social media or via any other Website, Cloud Storage or Platform.

11. Be aware of the seriousness of collusion and plagiarism. Do not post the answers to or feedback on assessments on social media, CILEX Law School Forums, any other Website or Platform.

12. You should remain vigilant about online safety. In particular:

- Check your social media privacy settings and consider what you share and with whom. In addition, you can complete the Right to Object Form on each social media channel to object to the data scraping of your account for the purposes of collating information for publicly accessible AI Platforms, which means that your information becomes publicly available worldwide.
- Use a strong and unique password containing at least 8 characters for all of your online accounts (with a combination of uppercase and lowercase letters, numbers and symbols), which must not be the same password that you use for other accounts (in particular, have different home and work account passwords), it should not contain any user account name or two consecutive letters of the user's name, any common dictionary words and do not use easily discoverable information, such as the name of favourite Sports Team, Date of Birth, Children's or Pet's names, etc. You can also use Multi-Factor Authentication, where available on Login options.
- You should use anti-virus software, a VPN and change your default password on your Wi-Fi access (you can also ask for your broadband provider for advice on creating separate home and work access to your Wi-Fi with different logins, if required) for IT Security.
- Please do not share your log in information or passwords and do not keep these in an easily accessible location. Secure Online Password Managers are available, if required.
- Be cautious about divulging information that could be used to steal your identity - protect your Personal Data (e.g., Phone Number, Address, Date of Birth, etc.) and your Special Categories of Personal Data. Where possible, it is not recommended to post photos of yourself online, including profile photos and in posts, with particular regard to online AI Data Scraping.
- Be cautious about what information you share with individuals that you have not met before.
- Remember to log out properly from a site, when you are finished, especially from a shared computer. You should also lock your screen, when you are away from your PC, Laptop, Tablet, Mobile Phone or other Device. You should also shut down your device, when you have finished using it to allow for Security and Software Updates.

Online Safety Resources:

Is your password strong enough and how long will it take to crack?

Enter a password on this website: [How Secure Is My Password? | Password Strength Checker | Security.org](#)

How do you know, if your information has been part of a registered Data Breach?

Enter your home email address or phone number onto this website: [Have I Been Pwned: Check if your email has been compromised in a data breach](#)

What to do, if you are a victim of Identity Theft?

Click on the link: [Identity theft | ICO](#)

13. When participating in an Online Webinar:

- Ensure that you use a professional name, when you enter the Webinar Room (this does not have to be your full name, for example, it could be your First Name and First Initial of your Surname). Check that you have not retained a nickname or designation that might appear unprofessional or cause offence to others. Please also be mindful of any uploaded profile photos, particularly, if it is not an uploaded professional photo of yourself i.e. a pet photo or an AI Generated Profile Photo, if your camera is switched off at any point.
- Check what you can see, when you first log in, as this is what others will see: be aware of any

personal photos or items in the background. Use the 'blur background option' to hide any background, if needed.

- Conduct yourself in a professional manner throughout the session:
 - Be punctual and courteous and turn your phone to silent.
 - Attend from a desk, table or other appropriate location.
- Mute your microphone, when not needing to talk to avoid any background noise.

14. If you have any queries about what amounts to Unacceptable Behaviour or if you wish to report any Unacceptable Behaviour, then you should contact the Designated Safeguarding Officer.

Cybercrime:

Cybercrime is becoming increasingly sophisticated, and learners may be targeted through scams, malicious software, identity theft or attempts to steal personal information.

Learners may experience:

- Phishing emails pretending to be employers, banks and other reputable organisations
- Fake apprenticeship or employment opportunities
- Identity theft
- Account hacking
- Financial scams
- Malware downloaded from unsafe websites
- Social media account compromise

How Staff Should Support Learners

Staff should:

- Encourage learners to use strong, unique passwords and Multi-Factor Authentication (MFA).
- Discuss the importance of protecting personal information online.
- Encourage learners to verify emails, messages and websites before responding.
- Signpost learners to trusted sources if they believe they have been targeted.
- Report concerns where cybercrime may place a learner at risk of harm or exploitation.
- Remind learners never to share passwords or verification codes.

Where appropriate, staff should encourage learners to report cybercrime to the relevant authorities and seek support from the organisation.

Deepfakes and AI-Generated Content:

Deepfakes are AI-generated or manipulated images, videos or audio recordings that appear genuine but have been altered to deceive viewers. Deepfakes are becoming increasingly realistic and may be difficult to identify.

Learners may encounter:

- Fake celebrity or public figure videos
- Manipulated social media content
- AI-generated voice messages

- False evidence shared online
- Deepfake images used for bullying or harassment
- Fake videos intended to spread misinformation

Staff should be alert to situations where deepfakes are used:

- As part of bullying.
- To harass or humiliate another learner.
- To damage someone's reputation.
- To impersonate individuals.
- To facilitate fraud or exploitation.

Any incident involving suspected deepfake abuse should be treated seriously and referred in line with safeguarding procedures.

Appendix 2: E-Safety Incident Report Form

This form should be emailed to: safeguarding@cilexlawschool.ac.uk

Details of the Incident

Date and Time of the Incident:

Name of the Person reporting the Incident:

Type of Incident:

- Data Protection and IT Security infringements, such as data breaches, unauthorised access to, loss of or sharing of Personal Data.
- Risk of being groomed or radicalised.
- Access to illegal, harmful or inappropriate website images, games or content.
- Cyber-Bullying.
- Plagiarism, Copyright and Intellectual Property Infringements.
(AI Hallucinations and AI Bias are also issues, when using AI Platforms.)
- Other (please specify).

Description of Incident:

Action Taken:

Outcome of Incident/investigation:

Appendix 3: Social Media Accounts - Right to Object to AI Data Scraping

AI Data Scraping to commence in 2024 on Meta owned Social Media Channels (affecting Personal and Business Social Media Accounts) and How to Protect your Personal/Business Data?

What is happening? Postponed initially from 26th June 2024 to September 2024 onwards, Meta will be utilising data scraping/collating your information from your personal and business social media accounts to be utilised by its AI Training Platform and Chatbot for future AI Features that will be publicly accessible, including the content of your social media channel. This includes Facebook and Instagram. LinkedIn also currently have plans to data scrape their personal and business accounts for the purposes of an AI Platform, please check the LinkedIn Privacy Policy for further information or online articles.

What information will be data scraped (collated) from your Social Media Account?

All information, including photos, tags to photos and your posts (whether you have posted publicly or to Friends/Contacts Only) and if you are mentioned in a post or feature in a photo that is published on other people's accounts. The only exception is the private messaging feature, when sending messages to friends or family (this is separate from your posts). Meta has updated their Privacy Policy reflecting the new changes, according to its email to users.

Why is this a problem?

- Meta is only relying only on Legitimate Interests, as their lawful basis for processing this personal data and they will not request the Consent of the Data Subject (access permission from you), as legally required in the UK Data Protection Legislation, before this data extraction. Whereas, Google and Microsoft typically require explicit opt-in from users, before incorporating their data into training processes, such as AI. Only Brazil has banned them from doing so and despite other Data Protection Supervisory Authority's raising objections (including the UK's ICO), they still plan on proceeding.
- The information collated will contribute to a publicly accessible AI Platform/Chatbot, which as with other examples, such as ChatGPT means that anything inputted/collated can be searched by other users worldwide becoming publicly available information.
- Photos can be used for AI Deepfakes and AI Generated Scams, such as voice and image cloning, creating a fake video version of yourself with audio and this also affects any video with audio that you have posted. There has also been a recent Mumsnet debate about posting photos of your children online, whereby the Police have agreed that this is not advisable for security reasons, including due to AI generated child pornography content.
- **Meta may still use your data to train its AI in some cases, whether you use its platforms or not. This will affect you, if you appear in or are mentioned in posts, photos and captions shared by any other personal or business account Instagram and Facebook Users.**
- Meta can utilise personal data for targeted advertising and to sell the personal data to third-parties for marketing purposes.
- For business information, including both personal and business social media accounts, this can become available to Competitors more easily and any other privacy concerns on obtaining your business-related content.

- Meta's AI development process lacks transparency. Ask yourself: Has the company made it clear exactly how your data is being used or what kind of AI models it contributes to?, which is applicable, when raising your objections. **You can only raise your objections in every account that you have under their “Right to Object Form” and there is no privacy setting that you can activate to prevent this data scraping.**

What can I do to protect my personal data and business-related data?

AI Governance is equally applicable now to both using a publicly accessible AI Platform, such as ChatGPT, Internet/Websites Content and now Social Media Channel Content, (where it is data scraped for the same purpose) and it is subsequently publicly available information: You should not input any Personal Data (including any Special Categories of Personal Data), any business confidential information, any photo or video without the written Consent of the Data Subject, a company logo or anything that is subject to Copyright or Intellectual Property Rights.

Delete any historical posts, photos or tags, that you do not wish to have data scraped/collated for this purpose.

Do you have Consent of the Data Subject to post a photo of someone else in your Social Media account or to mention them in a post?, if not, then it is advisable to delete this information.

Contact Meta to raise your Objections:

Under UK Data Protection Legislation, which is the Data Protection Act 2018, you have “Rights of the Individual”, such as the Right to Restrict Data Processing and the Right to Object to Data Processing”. Facebook or Instagram Users could express their concern about the lack of control over how their data, which is used in AI training. They could mention the potential for unforeseen consequences or misuse of their data in future applications, such as AI Tools that have been known to produce misinformation and even hatred in the past. You could enter: "I have the copyright to my posted data and I do not grant the right of use for AI applications" or "I generally feel uncomfortable at the thought of my data being used by an AI." You can mention that they do not have “Consent of the Data Subject”, which is the primary lawful basis required to process your Personal Data (including Special Categories of Personal Data) under the UK’s Data Protection Act 2018.

If you do not want your data to be used to train Meta's AI, you can object using a form, which takes less than 5 minutes to complete. However, Meta has hidden the form deep within several menus on a page that's poorly optimised for mobile phones and this may mean that many users are likely not to bother using it.

How to find the Form on Instagram and Facebook:

For Instagram:

- **Open your profile page and tap on the three-dash menu button in the corner to open the settings.**
- **Scroll all the way down and tap on "about".**
- **Then select "Privacy Policy" and find on the "Right to Object" link in the text box that appears near the top.**

You can fill out a short form on Instagram’s website, which asks for reasons why you want to opt

out, along with some personal information, such as your country of residence and email. [Instagram Help Centre](#)

For Facebook:

- **Open your profile page and (when in the browser) click on your profile photo at the top right or (when in the app) tap on the three dots on the right.**
- **Then select "Settings and Privacy" and then "Settings". Scroll down to the "Privacy Policy" section and click or tap on the "Right to Object" link in the text box.**

Once you get to this Objection Form, you'll then need to first enter your country of residence and an email address.

If you have several accounts with Meta and use different email addresses for each of them, you must fill in a separate form for each address.

You then must express your concerns in the field, where Meta asks how this processing affects you.

Meta will then judge, whether the reasons for the objection should be valued higher than its own business interests, the consumer protection experts say. However, there are initial reports from those requesting exemption are promising and Meta has accepted many of their objections without them having written a long justification.

ICO: It is recommended that, if you are unhappy with Meta's response, that you can register a complaint with the ICO (UK's Data Protection Supervisory Authority), along with the relevant information. They can investigate Meta's practices and potentially issue fines or enforcement.

Link: [Make a complaint | ICO](#)

Legal Action: You can also take personal/business legal action against a Social Media Provider, however, this would be expensive and you would be required first to notify your Social Media Provider of your objections and to have registered a complaint with the ICO, as a pre-requisite to this action.

Close your account/What's the alternative for a personal social media account?

You can also stop posting, opt to remove all content and then close the Social Media Account itself, prior to the commencement date. (i.e. for a Personal Social Media Account).

A possible secure alternative might be setting up a Friends and Family MS Teams Channel for MS Chat, whereby only the person setting it up requires an MS 365 account, as with MS Teams video calls, as you can send access to external email addresses (although, it would be advisable to keep up-to-date on any developments on MS Recall (where Microsoft are also looking to data scrape for the purposes of contributing content to AI Platforms), so you may also wish to look at other secure alternatives (please also note, that Slack has data scraping for AI purposes). A more secure alternative to WhatsApp, which is easily hackable with inadequate security (also owned by Meta) is a lesser-known competitor known as Signal, which has the most security, as an alternative Messaging App.

When using or registering for any Software or Application, including Social Media Channels, it is advisable to read their Privacy Policy, Terms of Use and to find out their IT Security and Data Breach record i.e. via an Internet search.

You should make sure that your Privacy Settings in your account are kept up-to-date,

according to your preferences and any subsequent changes that can be implemented by the Provider. Just because it is the most well-known App, it does not mean that it is the most secure application out of the comparable applications. You can also find comparable online security reviews of different brand Apps with the same or similar function/s online.