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 Pawned: 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.