Policy Name:	***E-Safety Policy and Procedure***
Policy Ref:	POL/ES/CLS/001
Who it applies to:	Learners, Employees, ASC.
Date of issue:	Version 0.3
Date last revised:	June 2023
Policy Type:	CLS
Policy Owner:	Head of Quality and Programme Compliance / Academic Director
Approved by:	SMT
Review date:	June 2024
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

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:

- Unauthorised access to / loss of / sharing of personal information
- Risk of being groomed or radicalised
- Access to illegal, harmful or inappropriate website images, games or content
- Online sexual harassment or abuse
- Cyber bullying
- Plagiarism and copyright infringement

CILEX | Law School

2. Purpose and Scope of Policy

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 is not limited to:

- email
- the internet
- the VLE (CLS Hub), associated forums and webinar rooms (Zoom)
- social networking sites and social mobile apps
- mobile phones
- MS Teams

This policy applies to all online behaviour by learners that is linked to 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 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 policy and procedures.

CILEX Law School cannot eliminate the risks associated with the use of technology but will address these risks through regular training and our e-safety guidelines (Appendix 1).

3. Roles and Responsibilities

3.1 Academic Director

The Academic Director will be responsible for overseeing the e-safety of CILEX Law School learners. Day to day responsibility for implementing and monitoring e-safety is delegated to the Head of Quality and Programme Compiance.

3.2 Head of Quality and Programme Compliance

The Head of Quality and Programme Compliance will be responsible for the implementation and monitoring of this policy. The Head of Quality and Programme Compliance will ensure that both staff and students have access to appropriate training in relation to e-safety.

3.3 Designated Safeguarding Officer (DSO)

3.3.1 The DSO will be trained in e-safety and be aware of potential issues which may arise from:

- Unauthorised access to / loss of/ sharing of personal information
- Risk of being groomed or radicalised
- Access to illegal, harmful or inappropriate website images, games or content
- Cyber bullying

3.3.2 The DSO will deliver staff development and training, record incidents, report any developments and incidents and 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 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 of ICT Policy

- E-safety is embedded in teaching, learning and assessment where appropriate
- Learners have an understanding of research skills and how to avoid plagiarism They 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
- They keep their log in details/passwords secure and confidential and 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 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 Designated Safeguarding Officer (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
- Staff discipline issues will be dealt with under the relevant staff policy
- Cybersecurity issues will be dealt with by the Information Technology Team and/or E Learning Manager depending on the nature of the issue.

5. Reporting Incidents

Incidents should be reported to the 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 Quality and Programme Compliance.

CILEX Law School will deal with e-safety incidents in the same way as safeguarding and Prevent issues and when appropriate will refer issues to:

- MASH (Multi Agency Support Hub)
- Police

6. Monitoring and Review of this Policy

The implementation of this policy will be monitored by the Head of Quality and Programme Compliance. E-safety incidents will be an integral part of the continuous safeguarding development, monitoring and review and 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 https://www.swgfl.org.uk/Staying-Safe
- SWGfL https://swgfl.org.uk/products-services/online-safety/resources/
- Cyber Aware Cyber Aware - NCSC.GOV.UK
- Safer Internet Day http://www.saferinternet.org/ww/en/pub/insafe/index.htm
- 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

8. Associated Policies

The following policies are associated with this policy:

- Safeguarding Policy and Procedure
- Prevent Policy
- Equality, Diversity, Inclusion Policy
- Accessibility Procedure
- Student Code of Conduct
- Learner Disciplinary Procedure
- Teaching, Learning and Assessment Policy
- Staff Grievance Procedure
- Staff Disciplinary Procedure
- CILEX Information Technology (IT) Policy
- 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 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 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:

- Cyberbullying
- 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 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

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 you post on social media can impact on your professional reputation: consider your cyber footprint. Prospective employers may check your social media profile. The posts you 'like' and organisations you follow may be used by others to form a judgement about you.

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

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

9. Do not share personal information in relation to a fellow student without their explicit consent. Do not name fellow students or staff on public forums/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; you should use the appropriate Complaints procedure instead.

10. Do not share any CILEX Law School materials or recordings of webinars on social media.

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.

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

- Check your social media privacy settings and consider what you share and with whom
- Use a strong and unique password for all of your online accounts (a combination of letters, numbers and symbols)
- Do not share your log in information or passwords, or keep these in an easily accessible location
- Be cautious about divulging information that could be used to steal your identity - protect your personal information (e.g. phone number, address, date of birth)
- Be cautious about what information you share with individuals that you have not met
- Remember to log out properly from a site when you are finished, especially from a shared computer

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). Check that you have not retained a nickname or designation that might appear unprofessional or cause offence to others.
- 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 you wish to report unacceptable behaviour, you should contact the Designated Safeguarding Officer.

Appendix 2: E-safety Incident Report Form

This form should be sent to safeguarding@cilexlawschool.ac.uk

Details of incident

Date and time of incident:

Name of person reporting the incident:

Type of incident:

- Unauthorised access to / loss of / sharing of personal information
- Risk of being groomed or radicalised
- Access to illegal, harmful or inappropriate website images, games or content
- Cyber bullying
- Plagiarism and copyright infringement
- Other (please specify)

Description of incident:

Action taken:

Outcome of incident/investigation: