Online Safety Policy

Expanse Learning Group

Oct 2024

Author:
Scott Roberts

Version:
6

This Policy was approved by:
Board of Directors on 18th October 2024

Date for Review:
October 2025

Document Name: Online Safety Policy **| Document Reference:** ELGR-DAMA-POL-0004
Release Date: October 2024 **| Review Date:** October 2025

Page 1 of 5

Online Safety Policy - ELGR-ITSM-POL-0004 - Exp.2025.10.v6.docx

1. Scope

This policy applies to:
- All staff at Expanse Learning with access to IT systems, whether on the premises or working remotely.
- The use of the internet, electronic communication devices (e.g., email, mobile phones, games consoles, social networking sites), and any systems that utilize the internet for connection and information sharing.

2. Introduction

Expanse Learning recognises the opportunities that new technologies bring to teaching and learning. Our approach involves implementing robust safeguards and educating staff and students on identifying and managing risks. This policy is part of our wider effort to ensure e-safety, complementing policies like Safeguarding and Child Protection, Social Networking, Anti-Bullying, and Disciplinary Policies.

As part of our duty to protect staff and students, we aim to promote safe digital practices and fulfil our broader duty of care. This policy should be read alongside other relevant policies.

3. Definition of E-Safety

The term e-safety is defined, for the purposes of this document as:

"The process of limiting the risks to children, young people and vulnerable adults when using Internet, Digital and Mobile Technologies (IDMTs) through a combined approach to policies and procedures, infrastructures and education, including training, underpinned by standards and inspection"

Young people's extensive use of e-technologies leaves no doubt over the importance of e-safety and the need for young people, and those who care for or work with them, to be able to take appropriate preventative action to minimise the associated risks.

These risks have been defined in various ways and are becoming more commonly categorised as follows:

	Content Child engages with or is exposed to potentially harmful content	**Contact** Child experiences or is targeted by potentially harmful *adult* content	**Conduct** Child witnesses, participates in or is a victim of potentially harmful *peer* conduct	**Contract** Child is party to or is exploited by potentially harmful contract
Aggressive	Violent, gory, graphic, racist, hateful, or extremist information and communication	Harassment, stalking, hateful behaviour, unwanted or excessive surveillance	Bullying, hateful, or hostile communication or peer activity e.g., trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, hacking, blackmail, security risks
Sexual	Pornography (harmful or illegal), sexualisation of culture, oppressive body image norms	Sexual harassment, sexual grooming, sextortion, the generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messaging, adverse sexual pressures§	Trafficking for purposes of sexual exploitation, streaming (paid-for) child sexual abuse
Values	Mis/disinformation, age-inappropriate marketing, or user-generated content	Ideological persuasion or manipulation, radicalisation, and extremist recruitment	Potentially harmful user communities e.g., self-harm, anti-vaccine, adverse peer pressures	Gambling, filter bubbles, micro-targeting, dark patterns shaping persuasion or purchase
Cross-cutting	**Privacy violations** (interpersonal, institutional, commercial) **Physical and mental health risks** (e.g., sedentary lifestyle, excessive screen use, isolation, anxiety) **Inequalities and discrimination** (in/exclusion, exploiting vulnerability, algorithmic bias/predictive analytics)			

4. Aims

This policy aims to:
- Ensure strong safeguards in IT systems.
- Promote safe and appropriate user behaviour.
- Secure storage and use of personal data in compliance with legal requirements.
- Educate staff and students on e-safety.
- Manage any e-safety incidents appropriately.

Document Name: Online Safety Policy **| Document Reference:** ELGR-DAMA-POL-0004
Release Date: October 2024 **| Review Date:** October 2025

Page 2 of 5

5. Outcomes

Security

Networks are protected using the latest security measures, including:
- Microsoft Defender for Endpoint
- Firewall with Web Content Filtering
- NetSupport School Tutor
- Network protected by Agilisys (Wigan Council's approved security provider)

Risk assessment

Risk assessments are carried out whenever new technologies or platforms are introduced.

Behaviour
- All users of technology adhere to the standards of behaviour set out in the IT Acceptable Use Policy.
- All users of IT adhere to IT Acceptable Use Policy and when using email, mobile phones, social networking sites, games consoles, chat rooms, video conferencing and web cameras, etc.
- Any abuse of IT systems and any issues of cyber bullying are dealt with seriously, in line with staff and student disciplinary procedures.
- Any conduct considered illegal is reported to the police.

Use of images and video
- The use of images or photographs is encouraged in teaching and learning, providing there is no breach of copyright or other rights of another person.
- Staff and students are trained in the risks in downloading, posting and sharing images, and particularly in the risks involved in posting personal images onto social networking sites.
- Staff provide information to students on the appropriate use of images, and on how to keep their personal information safe.
- Advice and approval from a senior manager are to be sought in specified circumstances or if there is any doubt about the publication of any materials.

Personal information
- Processing of personal information is done in compliance with the Data Protection Act 2018
- Personal information is kept safe and secure and is not passed on to anyone else without the express permission of the individual.
- No personal information is posted to the organisation's website/intranets without the permission of a senior manager.
- Staff always keep students' personal information safe and secure.
- When using an online platform, all personal information is password protected.
- All personal information sent electronically should follow the password protected and encrypted using Microsoft office 365 security.
- Every user of IT facility logs off on completion of any activity, or ensures rooms are locked if unsupervised, where they are physically absent from a device.
- Organisation mobile devices are encrypted, and password protected.
- Personal data no longer required, is securely deleted.
- Make sure you don't discuss sensitive information in inappropriate venues, e.g., public areas. When you take a phone call, ask the caller to confirm their personal information to you rather than you reading their details out loud.
- Only transfer personal information to removable media such as CDs, DVDs and memory stick if you have been authorised to do so. Unauthorised access to the information should be prevented using encryption. (taken from the Information Security Guide)
- Look after portable equipment such as laptops, iPad and memory stick. If you're travelling with them ensure you always keep them within your sight. Where possible attach a memory stick to a key ring.

Document Name: Online Safety Policy **| Document Reference:** ELGR-DAMA-POL-0004
Release Date: October 2024 **| Review Date:** October 2025

Page 3 of 5

Education and Training
- Staff and students are supported through training and education to develop the skills to be able to identify risks independently and manage them effectively.
- Student inductions and the tutorial programme contains sessions on e-safety.
- Students are guided in e-safety across the curriculum and opportunities are taken to reinforce e-safety messages.
- Students should discuss with their tutors when they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search.
- In classes, students are encouraged to question the validity and reliability of materials researched, viewed or downloaded. They are encouraged to respect the copyright of other parties and to cite references properly.
- Any new or temporary users receive training on the organisation IT system, they are also asked to sign the Acceptable Use Policy.

6. Incidents and response
- A clear and effective incident reporting procedure though Databridge is maintained and communicated to staff.
- Students should discuss with their teachers when they have concerns about an incident.
- Reports of e-safety incidents are acted upon immediately to prevent, as far as reasonably possible, any harm or further harm occurring.
- Action following the report of an incident might include disciplinary action, sanctions, reports to external agencies (e.g. the police), review of internal procedures and safeguards, tutor support for affected students, etc.

7. Responsibilities
The Executive Leadership Team are responsible for maintaining this policy and maintaining best practice in IT procedures and practices to manage any e-safety risks effectively.

The following are responsible for implementing it:
- Corporate Services for all e-safety matters in relation to staff.
- Teaching and Learning Staff for providing pastoral and practical support for students dealing with issues related to e-safety and for incorporating e-safety in student induction, supporting the tutorial scheme of work, and for providing an appropriate range of resources.
- All teachers for embedding e-safety education and practice into their teaching programme.
- All Heads of Departments for implementing good e-safety practice and safeguards consistent with this policy in their area of responsibility.
- The Safeguarding Team for overseeing and reviewing e-safety arrangements.
- All members of staff for staying alert to and responding appropriately to any potential or actual e-safety issue.

8. Legal Framework
- Racial & Religious Hatred Act 2006
- Sexual Offences Act 2003
- Police & Justice Act 2006
- Computer Misuse Act 1990 (s1-3)
- Communications Act 2003 (s127)
- Data Protection Act 2018
- Malicious Communications Act 1988 (s1)
- Copyright, Design & Patents Act 1988
- Public Order Act 1986 (s17-29)
- Protection of Children Act 1999 (s1)
- Obscene Publications Act 1959 & 1964
- Protection from Harassment Act 1997
- Regulatory of Investigatory Powers Act 2000

9. Monitoring arrangements
The impact of the policy will be monitored regularly with a full review being carried out at least once every year. The policy will also be reviewed where concerns are raised by the Safeguarding Officer, or where an e-safety incident has been recorded.

Document Name: Online Safety Policy **| Document Reference:** ELGR-DAMA-POL-0004
Release Date: October 2024 **| Review Date:** October 2025

Page 4 of 5

Impact of non-compliance:

Staff:	Disciplinary action
Student:	Suspension, Temporary Exclusion, Permanent Exclusion
Legislation/organisational:	Reputational damage, statutory and non-regulated compliance.
Compliance lead:	Headteacher/Director of Schools
Policy Reference:	ELGR-ITSM-POL-0004
Version:	6
Agreed policy location:	PeopleHR, Company Intranet and Webpage
Policy Schedule:	Annual
Does the policy require Governor approval?	No

Version Control

Version	Date	Revision	Review Date
1	01/03/2021	First Issue	28/02/2022
2	12/10/2021	Reviewed in-line with KCSIE 2021	11/10/2022
3	12/10/2022	Reviewed in-line with KCSIE 2022	11/10/2023
4	10/02/2023	Policy reviewed and security section 5 updated	10/02/2024
5	20/10/2023	Reviewed and updated	20/10/2024
6	11/10/2024	Updated	11/10/2025

Document Name: Online Safety Policy **| Document Reference:** ELGR-DAMA-POL-0004
Release Date: October 2024 **| Review Date:** October 2025

Page 5 of 5