

Local Procedure Title	Online Safety
Home/ School/ College	Aspris College North Wales
ACS Policy number and title	ACS 38 E-Safety
Local Procedure template reference	ACS LP 38
Local Procedure date	01.09.2026
Local Procedure review date	01.09.2027
Local Procedure Author(s)	Daniele Kenneough-Langford
Local Procedure Ratification	Checked and Approved by: Scott Preston

1. Purpose

Aspris College North Wales recognises that digital technologies are an integral part of modern learning, employment, communication and independent living.

This procedure aims to:

- promote safe, responsible and positive use of digital technologies;
- support learners to develop digital resilience and independence;
- protect learners, staff and visitors from online harm;
- ensure effective safeguarding arrangements are maintained;
- support preparation for adulthood through meaningful and supported use of technology.

This procedure should be read alongside safeguarding, behaviour, anti-bullying, data protection and acceptable use policies.

2. Context

As a specialist post-16 college, we support young people and young adults with a range of additional learning needs and disabilities.

We recognise that:

- technology can promote autonomy, communication, self-advocacy and social connection;
- learners may require varying levels of support to understand and manage online risks;
- previous experiences of trauma, exploitation, bullying or adverse childhood experiences may influence how individuals engage online;
- building knowledge, confidence and resilience is more effective than relying solely on restriction.

Our approach is based on trauma-informed and relational practice, balancing safety, wellbeing and independence.

3. Trauma-Informed Approach to Online Safety

When concerns arise regarding online activity, staff will:

Local Procedure Template

- remain calm, respectful and non-judgemental;
- seek to understand the purpose and context of the behaviour;
- recognise potential links to communication differences, unmet needs, past experiences or vulnerabilities;
- focus on support, education and risk reduction;
- work collaboratively with the learner and, where appropriate, families and professionals;
- involve learners in decisions affecting their access to technology wherever possible.

The college aims to create an environment in which learners feel safe to report mistakes, concerns or online incidents without fear of blame.

4. Roles and Responsibilities

Principal and Senior Leadership Team

Responsible for:

- ensuring effective online safety arrangements across the college;
- ensuring that filtering and monitoring systems remain effective;
- promoting a positive culture of digital safety;
- ensuring staff receive appropriate training.

Designated Safeguarding Person (DSP)

Responsible for:

- managing online safety concerns;
- reviewing online safety incidents;
- maintaining appropriate records;
- liaising with external agencies where required;
- overseeing risk management relating to online activity.

Staff

Responsible for:

- modelling safe and professional digital practice;
- challenging unsafe online behaviour appropriately;
- reporting concerns promptly;
- supporting learners to develop digital resilience.

Learners

Expected to:

- use technology responsibly and respectfully;
- report concerns or inappropriate content;
- respect the privacy and rights of others;
- follow acceptable use expectations.

5. Learner Access to Technology

As a post-16 provision, the college recognises that learners are developing independence and preparing for adulthood.

Access to personal devices will therefore be:

- proportionate;
- individualised;
- informed by risk assessment where necessary;
- regularly reviewed.

Restrictions on access will only be considered where there is a clearly identified safeguarding, welfare or educational need.

Where restrictions are required, they will be explained clearly to the learner and regularly reviewed to support progression towards greater independence.

6. Filtering and Monitoring

The college uses Aspris-approved filtering and monitoring systems to reduce the likelihood of access to harmful, illegal or inappropriate content.

Systems are designed to identify potential concerns relating to:

- safeguarding;
- exploitation;
- extremism;
- self-harm;
- cyberbullying;
- inappropriate content;
- online abuse.

Monitoring arrangements are used to support safeguarding and wellbeing and are carried out in accordance with data protection requirements.

Safeguarding alerts are reviewed by appropriate staff and acted upon proportionately.

7. Online Safety Education

Online safety education is embedded throughout the learner journey and preparation for adulthood curriculum.

Key themes include:

- digital citizenship;
- safe online relationships;
- social media safety;
- privacy and data protection;
- scams and online fraud;
- misinformation and disinformation;
- cyberbullying;
- consent and image sharing;
- online gaming;
- artificial intelligence and emerging technologies;
- healthy online behaviours and wellbeing.

Where concerns arise, targeted intervention and support will be provided.

8. Email and Digital Communication

College email accounts must be used appropriately and professionally.

Learners and staff should:

- protect passwords;
- avoid sharing personal information unnecessarily;
- report suspicious communications;
- not engage in harassment, bullying or discriminatory communication;
- comply with copyright and intellectual property requirements.

Communication between staff and learners must only take place through approved college systems.

9. Social Media

The college recognises that social media can play an important role in communication, learning and social connection.

Learners will be supported to:

- understand privacy settings;
- recognise risks associated with sharing personal information;

- identify unsafe or exploitative online behaviours;
- develop safe and respectful online relationships.

Staff must maintain professional boundaries and must not engage with learners through personal social media accounts.

10. Cyberbullying and Online Harm

The college does not tolerate cyberbullying or online harassment.

Concerns will be addressed through:

- safeguarding procedures;
- restorative conversations where appropriate;
- education and support;
- risk assessment and planning.

Responses will be proportionate, person-centred and trauma-informed.

11. Artificial Intelligence (AI)

The college recognises the growing role of artificial intelligence in education and everyday life.

Learners will be supported to:

- use AI tools responsibly;
- understand limitations and risks;
- verify information obtained from AI systems;
- recognise AI-generated content, images and misinformation.

Staff will promote ethical, safe and appropriate use of AI technologies.

12. Preventing Radicalisation and Exploitation

The college recognises that online platforms may be used to promote extremist views, exploitation, criminal activity and harmful ideologies.

Filtering, monitoring, staff vigilance and education programmes support the college's safeguarding responsibilities under Prevent and related Welsh safeguarding guidance.

Any concerns will be referred through safeguarding procedures.

13. Incident Management

Where online safety incidents occur:

- immediate risks will be managed;
- learner welfare will be prioritised;
- appropriate records will be maintained;
- families, carers and external agencies will be involved where appropriate;

Local Procedure Template

lessons learned will inform future support and risk management.
14. Monitoring and Review
This procedure will be reviewed annually or sooner if: - legislation changes; - safeguarding guidance changes; - significant online safety incidents occur; - college practice requires amendment.

Note: The corporate policy is currently entitled "ACS 38 E-Safety"; however, throughout this local procedure the term "Online Safety" is used to reflect current educational and safeguarding terminology within our setting context of a college within Wales.

Contents Checklist (Local Homes/ Schools/ Colleges may add additional items – this is a core list)			
Local responsibilities		Risk assessments	
Contact plans		Access to email	
Correspondence		Access to social media	
Access to telephones		Children and young people's own communication devices	
Record keeping		'Local Rules' for safe and sensible communications and social media use	
Monitoring arrangements			

Local Procedure Review History:

Date Reviewed	Reviewer	Summary of revisions