

Alternative Education – Online Safety Policy

1 Policy Summary

Approved by: Safeguarding Subgroup	Owned by: DSL
Approved date: 01/07/2026	Effective Date: 01/07/2026
Version: 2026.01	Review due: 01/07/2027
Policy Statement Youth Connect South West (YCSW) is committed to safeguarding children and young people from harm when accessing digital technology as part of its Alternative Education provision only. Online safety is recognised as a safeguarding matter and forms part of YCSW's wider duty to promote the welfare of children and young people. YCSW has regard to the principles and best practice contained within Keeping Children Safe in Education (KCSIE) 2025, adapting these proportionately to reflect the nature, size and educational model of its provision. While KCSIE is statutory guidance for schools and colleges, YCSW uses it as a recognised benchmark for safeguarding practice within its education provision.	
Purpose The purpose of this policy is to: • Set out YCSW's approach to managing the online safety of its staff, volunteers, young people, and visitors • Explain online systems that have been set up, how they work, and the allowed access/use • Detail all forms of digital connectivity in relation to our young people • Address actions that should be taken should there be any safeguarding concerns	
Scope This policy applies to:	

- All staff, volunteers, sessional workers and contractors involved in the delivery of YCSW's education provision
- All on-site educational activity delivered by YCSW

This policy applies only where digital technology is used as part of education delivery and does not extend to personal use of technology outside YCSW-led activity.

Related Policies and documents

This policy should be read in conjunction with YCSW's:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Acceptable Use expectations for staff and learners
- Managing Allegations Against Staff Policy
- Whistleblowing Policy
- Data Protection Policy

This policy has regard to recognised safeguarding guidance and legislation, including:

- Keeping Children Safe in Education (KCSIE) 2025, used by YCSW as a source of best practice and proportionate guidance for its education provision, particularly Part Two and Annex C
- Working Together to Safeguard Children
- Education Act 2002
- Children Act 1989 and 2004
- UK GDPR and Data Protection Act 2018

2 Policy Detail

2.1 Education Provision Context

YCSW's education provision operates within a supervised, small-group model and differs from mainstream school or college settings. In particular:

- Young people are not issued with individual laptops, IT accounts or email addresses by YCSW

- Technology use is occasional, purposeful and supervised by staff
- YCSW does not operate a virtual learning environment or remote learning platform

These contextual factors inform YCSW's proportionate approach to online safety, filtering and monitoring, as permitted under KCSIE.

2.1.1 Application of KCSIE

YCSW recognises that Keeping Children Safe in Education (KCSIE) is statutory guidance for schools and colleges. Although YCSW's education provision operates outside a mainstream school model, the organisation has adopted relevant KCSIE principles as recognised safeguarding best practice and applies them proportionately, taking account of the size, nature and delivery model of its provision.

2.2 Use of Devices and Technology

2.2.1 YCSW-owned Devices

Where YCSW laptops are used for educational purposes:

- Use is fully supervised by staff at all times
- Devices are shared and not allocated to individual learners
- Internet access is restricted where appropriate
- Laptops used for examinations do **not** have internet access enabled

Staff remain responsible for oversight of use and for intervening immediately where any concern arises.

2.2.2 Personal Devices

Young people are not required to use personal devices as part of YCSW's education provision. Where personal devices are present:

- They are not used as part of taught learning activity
- Staff maintain supervision and apply behavioural expectations

- Any safeguarding concerns arising from personal device use are managed in line with safeguarding procedures

2.3 Wi-Fi and Network Access

2.3.1 Staff Wi-Fi

YCSW operates a restricted staff Wi-Fi network:

- Access is limited and not available to all staff
- Log-in is managed by the administration team
- Passwords are not shared externally or with young people
- Appropriate filtering is applied to YCSW-managed networks

2.3.2 Public Wi-Fi

YCSW also provides a public Wi-Fi network to reflect the wider community use of its sites, including youth work, community activity and partner organisations.

- Public Wi-Fi may be accessed by visitors, contractors, partner agencies and young people using personal devices
- Public Wi-Fi is not used concurrently with unsupervised education provision
- Where education activity takes place in shared spaces, young people are escorted and supervised at all times

Public Wi-Fi access is not actively monitored, as it does not involve YCSW-owned devices, accounts or identifiable users. Risks are managed through supervision, staff vigilance and safeguarding procedures, reflecting the proportionate safeguarding principles outlined within KCSIE 2025.

2.4 Filtering and Monitoring

YCSW recognises the importance of effective filtering and monitoring arrangements and has adopted a proportionate approach informed by the best practice principles contained within KCSIE 2025.

- Filtering is applied to YCSW-managed networks and devices
- Routine individualised monitoring of online activity is not carried out, as young people are not issued with individual accounts or devices
- Staff supervision acts as the primary safeguarding control when technology is in use

This approach reflects the nature of YCSW's education provision and aligns with the proportionate filtering and monitoring principles described within KCSIE 2025.

2.5 Use of Third-Party and Partner Online Learning Platforms

As part of YCSW's Education provision, some learners may access online learning platforms provided by Bath College or other third-party education partners.

Where this occurs:

- Access to third-party platforms is arranged and managed by the external provider (for example Bath College), including the provision of user accounts, content, platform controls, filtering and monitoring
- YCSW does not administer, manage or technically control these platforms or associated learner accounts
- Use of third-party platforms by young people takes place under staff supervision where accessed on YCSW premises or as part of YCSW-led education activity

YCSW's safeguarding responsibility in relation to third-party online learning focuses on:

- Ensuring staff supervision and appropriate support for learners when accessing third-party platforms as part of education delivery
- Maintaining vigilance for safeguarding concerns arising from online activity, including exposure to harmful content, inappropriate contact or distress
- Reporting and escalating any concerns in line with YCSW's Safeguarding and Child Protection Policy
- Liaising with Bath College or the relevant provider where safeguarding or online safety concerns arise in relation to their systems

Responsibility for the technical operation, filtering, monitoring and data management of third-party learning platforms remains with the provider operating those systems.

2.6 Education, Training, and Awareness

Online safety is addressed through:

- Safeguarding training for all staff, including online risks and indicators of harm
- Clear expectations around professional boundaries and acceptable use of technology
- Staff awareness of how to identify, respond to and report online safety concerns

Young people are supported to understand safe and appropriate behaviour where technology is used as part of education activity.

2.7 Safeguarding Concerns and Reporting

Any online safety concern, disclosure or incident must be:

- Reported immediately to the **Designated Safeguarding Lead (DSL)** or Deputy DSL
- Recorded in line with YCSW's safeguarding procedures

Concerns may include, but are not limited to:

- Exposure to harmful or age-inappropriate content
- Online grooming or exploitation
- Cyberbullying or harassment
- Inappropriate online contact involving staff or other adults

Where concerns relate to the conduct of staff or volunteers, these will be managed in line with YCSW's Managing Allegations and Whistleblowing procedures.

2.8 Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) has overall responsibility for online safety within the education provision
- Senior leaders ensure that appropriate arrangements, training and oversight are in place
- Trustees provide strategic oversight and seek assurance that online safety arrangements remain proportionate, effective and informed by recognised safeguarding best practice, including KCSIE 2025.
- All staff are responsible for maintaining vigilance, supervising technology use and acting on concerns

3 Compliance & Enforcement

In the event that misconduct is discovered as a result of any investigation under this policy, the disciplinary policy and procedure will be invoked in addition to any external measures.

4 Review and Updates

This policy is reviewed annually, or sooner if required due to:

- Changes to KCSIE or other safeguarding guidance
- Changes to YCSW's education provision or delivery model

- Learning from safeguarding incidents, complaints or audits
- Trustees receive assurance that online safety arrangements within the education provision remain effective, proportionate and aligned with recognised safeguarding best practice, including the principles set out in KCSIE 2025.