Acceptable use policy for IT

Reviewed by:	Richard Fihosy and Claire Ames
Policy Commencement Date:	02.10.2021
Ratified by:	Provision Manager and DSL
Review:	Annual
Next Review:	Autumn Term 2026
Review Date 08.03.24 Richard Fihosy	Page and Sections Page 1 - Former Director's name was deleted. Any reference to "The Responsible Body" has been replaced with "AS2Educate Directors" Page 2 - Responsibilities. DSL has been changed to "Claire Ames" Any reference to "DSP" has been changed to "DSL"
Aug 25	Full Policy Review

Introduction

AS2Educate recognises that internet, mobile and digital technologies provide vital learning, communication, and developmental opportunities for young people—when used safely and appropriately. In today's digital landscape, online presence and reputation directly impact young people's future personal, academic, and economic success.

As a trauma-informed provision, we recognise that some young people may experience challenges with emotional regulation, attention, and boundaries. Therefore, online safety is embedded within a relational, strengths-based approach that helps young people feel empowered, not punished. Staff respond to incidents with curiosity and compassion while maintaining clear and consistent boundaries.

AS2Educate is committed to ensuring all young people, staff, the Provision Manager, and families understand digital risks, receive regular updates, and are supported to use technologies in a safe, ethical, and legally compliant manner.

We also recognise that children with SEND, social care involvement, or trauma backgrounds may be especially vulnerable to online harms. Staff are trained to provide repeated teaching, visual aids, and contextualised guidance to support secure, developmentally appropriate learning.

Responsibilities

The Provision Manager holds ultimate responsibility for implementing, embedding, and monitoring this Online Safety Policy. The Designated Safeguarding Lead (DSL), Claire Ames, and the Provision Manager oversee online safety, ensuring incidents are addressed in line with KCSiE 2025.

- All breaches must be reported via email to the Provision Manager.
- Any breach involving actual or potential risk to a child must also be reported immediately to the DSL.
- Concerns about staff conduct (including the Provision Manager) must be reported to the appropriate local authority officer or SEND officer.

Application

This policy applies to:

- Young people
- Parents/carers
- Teaching and support staff
- The Responsible Body
- Visitors and volunteers
- External agencies using AS2Educate facilities

Policy and Procedure

AS2Educate expects all members of its community to use digital technologies exclusively for appropriate and educational purposes, with due regard to safeguarding legislation, ethical behaviour, and wellbeing.

AS2Educate staff are provided with AS2-issued laptops. These devices must be used solely for AS2Educate business, and must not be used for any second jobs, freelance work, or unrelated employment. Misuse will be treated as a disciplinary matter.

Email Use

- Staff must use AS2 email accounts for all official communication.
- Personal accounts must never be used to contact pupils or families.
- Staff and young people must report suspicious emails to the Provision Manager.
- All emails must be respectful and non-threatening—cyberbullying is never tolerated.

Site Use & Downloading

- All apps and websites must be previewed by staff before use with young people.
- Google SafeSearch, filtered tools, or appropriate age-rated content must be used.
- Downloads must be relevant, legal, and free of malware.

Prohibited Activity

The following are strictly prohibited:

- Accessing, storing, or sharing illegal or indecent content
- Promoting hate, discrimination, violence, extremism, or harmful behaviours
- Using AS2Educate Wi-Fi or devices for private business or second jobs
- Accessing others' files without permission
- Publicly criticising AS2Educate or its staff online
- Revealing confidential student/staff information

Where an AS2-issued laptop is provided, only this device may be used to conduct AS2 business, both inside and outside of work.

All serious breaches will be reviewed with the DSL and reported to authorities if necessary.

Storage of Images

- Images/videos of students are can be taken on AS2 employees phones to take relevant curriculum based photos/ videos of students and upload these onto the AS2 secure drive at the end of each working day. Images will then be permanently deleted from personal devise.
- Consent is sought at induction and recorded.
- Only secure storage systems (e.g., approved cloud services) may be used.
- Parents/carers must not take images of children other than their own, whether onsite or offsite.

Use of Mobile Devices

- Staff may use personal phones **only** in the office or outside areas.
- If calls to parents/carers are necessary (e.g., attendance support), they must be logged in the young person's daily notes.
- Young people must hand in phones upon arrival. These are securely stored until the end of the session.
- No staff, parent, or pupil may use a mobile device to record images or audio without express written consent from the Provision Manager.

Staff and visitors must remain aware that trauma-experienced young people may be disproportionately affected by covert recordings, surveillance, or breaches of trust.

New Devices & Technology

- New personal or educational tech must be risk-assessed and approved before use.
- This includes VR headsets, smart watches, and consoles.
- Parents and carers should not assume permission is granted—approval must be sought in advance.

Reporting Concerns

- Any exposure to harmful content must be reported to a member of staff or DSL immediately.
- Staff must respond calmly and supportively, recognising the potential distress involved.
- Where there's risk of significant harm, safeguarding procedures will be activated.

Curriculum

Our online safety curriculum aligns with KCSiE 2025, PSHE, and RSE guidance. Teaching focuses on:

- Digital citizenship, resilience, and boundaries
- Navigating peer pressure and online reputations
- Critical thinking (e.g., fake news, online manipulation)
- Consent, privacy, and body autonomy online
- Exposure to extremism, violence, or abuse
- Understanding emotional triggers linked to online experiences
- Trauma-informed education around cyberbullying and digital exploitation

Staff Responsibilities

All staff receive annual online safety training, which includes trauma-informed strategies.

- All new staff sign the Acceptable Use Agreement
- Training is recorded in safeguarding logs

- Staff are encouraged to model emotionally regulated, respectful online behaviour

Parent & Carer Partnership

AS2Educate works proactively with families to promote safe technology use:

- Newsletters with online safety updates
- Advice on monitoring apps, setting boundaries, and using filters
- Encouragement to talk openly about risks and digital wellbeing
- Emphasis on co-regulation, empathy, and connection, not just restrictions

Device Monitoring – SENSO

To enhance safeguarding and promote a safe online learning environment, AS2Educate applies SENSO monitoring software to all student Chromebooks issued by the provision.

- SENSO enables real-time monitoring, keyword alerts, and usage tracking in line with KCSiE 2025 requirements for digital safety.
- The software helps identify potential safeguarding concerns such as online bullying, grooming, self-harm, extremism, or inappropriate searches.
- Monitoring is overseen by the Provision Manager and Designated Safeguarding Lead, with alerts reviewed and escalated where appropriate.
- Students and parents are made aware of this monitoring as part of induction and through the Acceptable Use Agreement.
- The use of SENSO is trauma-informed: staff are trained to respond proportionately and supportively if monitoring triggers a safeguarding response.

Monitoring and Review

- All breaches must be logged and reviewed with the DSL or Provision Manager.
- Incidents involving young people or staff are recorded, acted upon, and shared with the Responsible Body.
- If concerns are raised about the Provision Manager, they will be escalated to the child's SEND officer or external safeguarding partner.