

Digital Safety, Acceptable Use and Professional Online Conduct Policy – August 2026

Contents

Introduction	3
Purpose	4
Scope	4
Principles	5
Roles and Responsibilities	5
Provision Manager and SLT	5
Designated Safeguarding Lead (DSL)	5
All Staff	6
Learners	6
Parents and Carers	6
Whole-Provision Approach	7
Digital Safeguarding	7
Digital Safety Education	8
Filtering and Monitoring	9
SENSO Monitoring	10
Supervision of Technology	10
Acceptable Use of Technology	10
Staff Use of Technology	11
Email	11
Internet Use	12
Downloads and Software	12
Password Security	12
Cloud Storage and Data	13
Artificial Intelligence (AI)	13
Cyber Security	14
Data Protection and Confidentiality	14
Staff Use of Mobile Devices, Images, Social Media and Professional Conduct	14
Use of Mobile Devices	14
Photography, Video and Audio Recording	15
Social Media and Online Professional Conduct	16
Professional Boundaries	17

Professional Reputation	17
Confidentiality	17
Online Conduct	18
Monitoring and Compliance	18
Remote Learning and Online Meetings	18
Reporting Online Safety Concerns	19
Behaviour and Consequences	19
Monitoring, Review and Continuous Improvement.....	20
Appendix 1	21

Introduction

AS2Educate is committed to safeguarding and promoting the welfare of every child and young person. Digital technology is an integral part of education, communication and daily life, providing significant opportunities for learning, personal development and inclusion. However, it also presents safeguarding, wellbeing, privacy and cyber security risks that must be effectively managed.

Online safety is recognised as a safeguarding issue rather than simply an information technology issue. Protecting children from online abuse, exploitation, bullying, harmful content and inappropriate contact forms part of AS2Educate's wider safeguarding responsibilities.

As a specialist provision working with children and young people who may have additional vulnerabilities, including special educational needs, disabilities, trauma, adverse childhood experiences or social care involvement, AS2Educate recognises that some learners may be at greater risk of online harm and may require additional support, supervision and education to remain safe.

AS2Educate is committed to creating a positive digital culture where technology is used safely, responsibly and ethically. We aim to promote digital resilience, support responsible online behaviour and develop the knowledge and skills that enable children and young people to participate safely in an increasingly digital world.

All adults working at or on behalf of AS2Educate have a professional responsibility to:

- safeguard children whilst using digital technology;
- maintain appropriate professional boundaries online;
- model safe, respectful and responsible digital behaviour;
- protect confidential information;
- comply with data protection and cyber security requirements; and
- report concerns promptly in accordance with the Safeguarding and Child Protection Policy.

This Policy combines AS2Educate's previous Acceptable Use of IT Policy, E-Safety Policy and Social Networking Policy into one comprehensive framework governing the safe use of technology and professional online conduct.

This Policy should be read alongside:

- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Low-Level Concerns Policy
- Whistleblowing Policy
- Behaviour & Anti-bullying Policy
- Equality, Diversity and Inclusion Policy
- GDPR & Privacy Policy
- Health and Safety Policy

Purpose

The purpose of this Policy is to:

- safeguard children and young people from online abuse, exploitation and harm;
- promote the safe, responsible and ethical use of digital technology;
- establish clear expectations for acceptable use of AS2Educate systems and devices;
- ensure all staff maintain appropriate professional boundaries when communicating online;
- promote positive digital citizenship and respectful online behaviour;
- protect confidential information and personal data;
- minimise cyber security risks;
- provide clear procedures for reporting concerns;
- ensure effective filtering, monitoring and supervision of digital activity;
- support compliance with statutory safeguarding responsibilities; and
- foster a culture where online safety is everyone's responsibility.

Scope

This Policy applies to everyone working for or on behalf of AS2Educate, including:

- employees;
- agency workers;
- volunteers;
- apprentices;
- students on placement;
- work experience students;
- contractors;
- visitors using AS2Educate technology;
- external professionals working within the provision; and
- learners accessing AS2Educate digital systems or devices.

The Policy applies whenever technology is used:

- on AS2Educate premises;
- during educational visits;
- whilst working remotely;
- during home learning;
- using AS2Educate devices;
- using personal devices for authorised AS2Educate business;
- whilst accessing AS2Educate systems;
- when communicating with members of the AS2Educate community; and
- where online conduct could reasonably impact the safety, wellbeing or reputation of AS2Educate.

The expectations within this Policy apply both during and outside working hours where conduct could affect professional relationships, safeguarding responsibilities or public confidence in AS2Educate.

Principles

AS2Educate is committed to ensuring that digital technology is used in ways that are:

- safe;
- lawful;
- respectful;
- inclusive;
- proportionate;
- transparent;
- secure;
- professionally accountable; and
- centred on the welfare of children and young people.

All decisions relating to online safety will place the best interests of the child at the centre of decision making.

Technology should support learning, communication and wellbeing while protecting children from foreseeable harm.

AS2Educate recognises that effective online safety requires a whole-provision approach involving leadership, staff, learners, families and external partners.

Roles and Responsibilities

Provision Manager and SLT

The Provision Manager and SLT have overall responsibility for implementing this Policy and ensuring compliance across AS2Educate.

This includes:

- promoting a positive culture of digital safety;
- ensuring all staff understand their responsibilities;
- overseeing acceptable use of technology;
- ensuring appropriate cyber security arrangements are maintained;
- ensuring digital systems remain fit for purpose;
- overseeing investigations into breaches of this Policy;
- ensuring appropriate disciplinary action is taken where necessary;
- ensuring appropriate records are maintained; and
- ensuring significant incidents are appropriately escalated to the Provision Manager and, where required, relevant external safeguarding, regulatory or commissioning bodies..

Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead has strategic responsibility for online safeguarding and will:

- oversee online safety as part of the wider safeguarding framework;
- manage safeguarding concerns arising from online activity;
- oversee filtering and monitoring arrangements alongside the Provision Manager;

- review safeguarding alerts generated through monitoring systems;
- ensure online safeguarding incidents are appropriately recorded;
- liaise with Children's Social Care, the Police, the Local Authority and other agencies where required;
- support staff managing online safeguarding concerns;
- monitor emerging online risks;
- contribute to staff training; and
- promote safe online practice across the provision.

All Staff

Every member of staff has a responsibility to:

- safeguard children whilst using technology;
- maintain professional boundaries online;
- model safe and respectful digital behaviour;
- use AS2Educate technology responsibly;
- comply with this Policy;
- protect confidential information;
- follow cyber security procedures;
- report safeguarding concerns immediately;
- report any online safety incidents, cyber security concerns or data breaches promptly;
- challenge inappropriate online behaviour where appropriate; and
- complete all required online safety and safeguarding training.

Staff must recognise that safeguarding responsibilities apply equally to online and offline environments.

Learners

Learners are expected to:

- use technology safely, respectfully and responsibly;
- follow staff instructions;
- use AS2Educate devices only for authorised educational purposes;
- respect the privacy and rights of others;
- protect passwords and personal information;
- report anything online that makes them feel unsafe, worried or uncomfortable;
- comply with the Behaviour Policy and Acceptable Use Agreement; and
- contribute to maintaining a safe and respectful online environment.
- Learners will receive regular education to develop their digital literacy, resilience and understanding of online risks.

Parents and Carers

AS2Educate recognises that parents and carers play a vital role in promoting children's online safety.

Parents and carers are encouraged to:

- work in partnership with AS2Educate to promote safe technology use;
- reinforce online safety messages at home;

- supervise age-appropriate technology use;
- report concerns promptly;
- support the expectations outlined within this Policy.
- AS2Educate will provide information, guidance and signposting to support families in promoting safe and healthy digital habits.

Whole-Provision Approach

Online safety is everyone's responsibility.

Effective safeguarding depends upon:

- strong leadership;
- clear professional expectations;
- effective filtering and monitoring;
- active supervision;
- positive relationships;
- ongoing education;
- partnership working with families;
- proportionate responses to concerns; and
- a culture in which children and adults feel confident to speak up.

AS2Educate is committed to maintaining a psychologically safe environment in which concerns about online safety, cyber security or professional conduct can be raised without fear of blame or reprisal and will be managed in accordance with the Safeguarding, Low-Level Concerns and Whistleblowing Policies.

Digital Safeguarding

Online safety forms an integral part of AS2Educate's safeguarding responsibilities. The risks children experience online are constantly evolving and may occur through social media, gaming platforms, messaging applications, artificial intelligence, live streaming, online communities and other digital technologies.

AS2Educate recognises that online risks may occur both within and outside the provision and that incidents occurring away from AS2Educate can have a significant impact on a child's welfare, education and wellbeing.

Children attending AS2Educate may be particularly vulnerable to online harm due to their age, special educational needs and disabilities (SEND), previous trauma, social care involvement, mental health needs or communication difficulties. Consequently, online safety is embedded throughout safeguarding practice and education.

Staff will remain alert to signs that a child may be experiencing online harm, including changes in behaviour, emotional wellbeing, attendance, relationships or engagement with learning.

Online safeguarding concerns may include, but are not limited to:

- online grooming;
- child sexual exploitation;
- child criminal exploitation;
- coercion or manipulation;
- cyberbullying;
- online harassment;
- sextortion;
- financially motivated sexual extortion (sextortion);
making or sharing nudes or semi-nudes and self-generated intimate images;
- image-based abuse, including non-consensual intimate imagery, digitally manipulated imagery, deepfakes and AI-generated sexual content;
- online abuse within intimate relationships;
- radicalisation or exposure to extremist material;
- harmful online challenges;
- violent or distressing content;
- pornography;
- gambling;
- misinformation or disinformation;
- online fraud or scams;
- identity theft;
- excessive or compulsive technology use; and
- any activity that places a child at risk of harm.

Where online concerns indicate that a child may be suffering, or is likely to suffer, significant harm, staff must follow the Safeguarding and Child Protection Policy immediately.

Digital Safety Education

AS2Educate provides age, ability and developmentally appropriate education to help learners develop the knowledge, skills and confidence needed to navigate the online world safely.

Online safety education is embedded throughout the curriculum and reinforced through daily interactions, pastoral support and safeguarding practice.

Teaching includes:

- staying safe online;
- protecting personal information;
- healthy online relationships;
- respectful communication;
- recognising online abuse;
- identifying grooming and exploitation;
- consent and digital boundaries;
- cyberbullying;
- reporting concerns;
- misinformation and fake news;
- digital footprints and online reputation;
- privacy settings;

- gaming safety;
- live streaming;
- social media;
- artificial intelligence, including the safe and responsible use of generative AI, AI-generated content, manipulated imagery and deepfakes;
- image-based abuse and the making or sharing of nudes or semi-nudes, taught in an age and developmentally appropriate way; scams and phishing;
- healthy screen use; and
- digital wellbeing.

Learning is adapted to meet individual needs and takes account of SEND, communication differences and trauma-informed approaches.

Filtering and Monitoring

AS2Educate recognises that effective filtering and monitoring systems are an essential safeguarding measure and are implemented in accordance with the Department for Education Filtering and Monitoring Standards.

Filtering and monitoring arrangements are designed to:

- reduce exposure to harmful or inappropriate material;
- identify safeguarding concerns at an early stage;
- support staff supervision;
- promote safe internet use; and
- protect both learners and staff.

Filtering and monitoring arrangements will be formally reviewed at least once every academic year, and sooner where there is a significant safeguarding incident, change to technology, identified weakness or other reason to consider whether the arrangements remain appropriate.

The review will include checks that filtering and monitoring arrangements are operating effectively on internet-connected devices and across relevant locations within AS2Educate. A record of these checks and reviews will be maintained.

The Provision Manager and Designated Safeguarding Lead will ensure that relevant staff understand the filtering and monitoring arrangements, their responsibilities within them, and how concerns or identified weaknesses should be escalated.

Monitoring systems support safeguarding but do not replace professional curiosity, effective supervision or staff vigilance.

Staff remain responsible for actively supervising children whenever digital technology is being used. Digital monitoring tools support, but do not replace, effective staff supervision, professional judgement or safeguarding responsibilities.

SENSO Monitoring

AS2Educate uses SENSO monitoring software across all provision-issued learner laptops.

SENSO provides safeguarding monitoring through:

- real-time screen visibility;
- internet activity monitoring;
- application monitoring;
- keyword alerts;
- safeguarding notifications;
- inappropriate content alerts;
- attempted access to blocked material;
- search monitoring; and
- device usage reporting.

Alerts generated through SENSO are reviewed by the Provision Manager and the Designated Safeguarding Lead.

Where alerts indicate possible safeguarding concerns, an immediate risk assessment will be undertaken and action taken in accordance with the Safeguarding and Child Protection Policy.

Monitoring information will only be accessed by authorised staff and managed in accordance with UK GDPR and the Data Protection Act 2018.

Students and parents/carers are informed during induction that provision-issued devices are monitored for safeguarding purposes.

Supervision of Technology

Children using digital technology remain under the supervision of staff at all times.

Staff are expected to:

- actively supervise learners using technology;
- remain aware of learner activity;
- intervene where inappropriate use is identified;
- encourage safe online behaviours;
- reinforce digital safety expectations;
- report concerns promptly; and
- maintain professional curiosity where behaviour causes concern.

Where a learner accidentally accesses inappropriate content, staff will respond calmly and supportively whilst taking appropriate safeguarding action.

Children should never fear reporting accidental exposure to harmful material.

Acceptable Use of Technology

Technology provided by AS2Educate exists primarily to support education, safeguarding and the effective operation of the provision.

All users are expected to use technology responsibly, safely and lawfully.

Use of AS2Educate technology must always be consistent with:

- safeguarding responsibilities;
- professional standards;
- confidentiality;
- data protection legislation;
- cyber security requirements; and
- this Policy.

Staff Use of Technology

Staff are issued with AS2Educate devices to undertake their professional duties. Provision-issued equipment must only be used for authorised AS2Educate business.

Staff must not use AS2Educate equipment for:

- secondary employment;
- freelance work;
- personal business activities;
- illegal activity;
- political campaigning;
- accessing inappropriate material; or
- any activity likely to bring AS2Educate into disrepute.

Where staff are issued with an AS2Educate laptop, this should normally be the only device used for undertaking AS2Educate work.

Any exception must be authorised by the Provision Manager.

Email

All staff must use their AS2Educate email account for all work-related communication.

Staff must:

- use only their AS2Educate email address when communicating with students, parents/carers, professionals or colleagues regarding AS2Educate business;
- never use personal email accounts to conduct AS2Educate business or communicate with students or families;
- ensure all emails are professional, respectful, factual and appropriate;
- check recipient details carefully before sending confidential information;
- report suspicious, phishing or malicious emails immediately to the Provision Manager;
- use secure methods when sending personal or sensitive information in accordance with the Data Protection Policy.

Staff must not download, copy, forward, disclose, store or share AS2Educate information, student records, safeguarding information or any other confidential organisational data with third parties or external individuals for personal use or any purpose not directly connected with their authorised role. This includes sending information to personal email accounts,

saving it to personal cloud storage or external devices, or sharing it via personal messaging applications or social media.

Any accidental disclosure or suspected data breach must be reported immediately in accordance with the Data Protection Policy and Information Security procedures.

Internet Use

Internet access is provided for educational and professional purposes.

Users must not:

- intentionally access illegal material;
- Users must not intentionally access, create, download, store, share or distribute illegal sexual imagery, child sexual abuse material, non-consensual intimate imagery or other unlawful content.
- access extremist material;
- promote discrimination or hatred;
- attempt to bypass filtering systems;
- access pornography;
- download unlicensed software;
- undertake illegal file sharing; or
- engage in unlawful online activity.

Any accidental access to inappropriate material must be reported immediately.

Downloads and Software

Only authorised software may be installed on AS2Educate devices.

Users must not install:

- unauthorised applications;
- browser extensions;
- VPN software;
- executable files;
- games;
- cryptocurrency software; or
- software that presents cyber security risks.

Downloads must originate from trusted and legitimate sources.

Password Security

Users are responsible for protecting their login credentials.

Passwords should:

- be unique;
- be difficult to guess;
- never be shared;
- never be written where others can access them; and
- be changed immediately if compromised.

Multi-factor authentication (MFA) must be enabled for staff accounts accessing cloud-based or remotely accessible AS2Educate systems where the system supports MFA. Staff must not disable or attempt to circumvent MFA or other security controls. Users must lock devices whenever they are left unattended.

Cloud Storage and Data

Confidential information must only be stored using approved AS2Educate systems.

Staff must not store confidential information on:

- personal cloud storage;
- unauthorised USB devices;
- personal computers;
- personal email accounts; or
- unapproved applications.

All personal data must be handled in accordance with UK GDPR and AS2Educate's Data Protection Policy.

Artificial Intelligence (AI)

AS2Educate recognises that artificial intelligence is increasingly used within education and professional practice.

Staff may use approved AI tools to support planning, administration and resource development where appropriate.

However, staff must never enter into AI systems:

- identifiable pupil information;
- safeguarding records;
- confidential staff information;
- personal data;
- sensitive organisational information; or
- information protected by confidentiality obligations.

AI-generated content must always be reviewed for:

- accuracy;
- safeguarding implications;
- bias;
- suitability;
- copyright; and
- educational appropriateness.

Professional judgement always remains the responsibility of the member of staff.

AS2Educate recognises that artificial intelligence may also create or amplify safeguarding risks. These may include the creation or manipulation of sexual or intimate imagery, deepfakes, impersonation, bullying or harassment, grooming, scams and financial

exploitation, misinformation or disinformation, harmful or inappropriate chatbot interactions, and the generation or distribution of harmful content.

Any use of AI that raises a concern about the safety or welfare of a child must be treated as a safeguarding matter and reported immediately to the DSL or DDSL in accordance with the Safeguarding and Child Protection Policy.

Learners may only use AI tools where authorised and supervised by staff for educational purposes.

AI must not be used to make safeguarding decisions, behavioural decisions or professional judgements without appropriate human oversight..

Cyber Security

Everyone has a responsibility to protect AS2Educate from cyber threats.

Staff must:

- remain vigilant to phishing attempts;
- report suspicious emails immediately;
- protect passwords;
- lock devices when unattended;
- install updates when instructed;
- use approved software only;
- avoid unknown USB devices;
- report lost or stolen devices immediately;
- report suspected cyber-attacks without delay; and
- comply with all cyber security procedures.

Cyber security incidents will be managed in accordance with AS2Educate's Incident Management and Data Protection procedures.

Data Protection and Confidentiality

All users must protect confidential information obtained through their work or education. Information relating to children, families, colleagues or AS2Educate must only be accessed where there is a legitimate professional reason.

Information must never be disclosed through digital technology without appropriate authority.

Any actual or suspected data breach must be reported immediately to the Provision Manager.

Staff Use of Mobile Devices, Images, Social Media and Professional Conduct

Use of Mobile Devices

AS2Educate recognises that mobile devices are an important part of everyday life. However, their use must never compromise safeguarding, confidentiality, professional boundaries or the welfare of children and young people.

Staff must ensure that the use of mobile devices complies with this Policy, the Staff Code of Conduct, the Safeguarding and Child Protection Policy and the Data Protection Policy.

Staff must:

- use personal mobile phones only during breaks or in designated staff areas unless required for authorised educational or safeguarding purposes;
- keep personal mobile phones secure at all times whilst on site;
- maintain professional boundaries when using mobile devices;
- ensure any communication with parents, carers or professionals is undertaken using authorised AS2Educate communication methods wherever possible;
- record any authorised telephone conversations relating to students within the student's record.

Staff must not:

- use personal mobile phones to communicate directly with students;
- use personal messaging applications (including WhatsApp, Messenger, Snapchat, Instagram, Signal or similar platforms) to communicate with students or their families unless specifically authorised by the Provision Manager in exceptional circumstances;
- make audio or video recordings within the provision without authorisation;
- allow personal use of mobile devices to interfere with supervision of students.

Students are expected to hand mobile phones to staff upon arrival. Devices will be stored securely and returned at the end of the session unless alternative arrangements have been agreed.

Visitors may be asked to restrict the use of mobile devices whilst on site where this is necessary to protect confidentiality and safeguarding.

Photography, Video and Audio Recording

Photographs and videos play an important role in celebrating achievement, recording learning and supporting assessment. However, they must always be taken, stored and used safely.

Images or recordings of students may only be taken:

- for legitimate educational, safeguarding or promotional purposes;
- where appropriate consent has been obtained in accordance with the Data Protection Policy;
- using authorised AS2Educate devices wherever possible.

Where an AS2Educate mobile phone has been issued, this should always be the first device used for taking photographs or videos for educational purposes. AS2Educate mobile phones are provided specifically to support curriculum activities, evidence of learning, safeguarding and other authorised provision activities.

Where an AS2Educate mobile phone is unavailable or its use is impracticable, staff may use their personal mobile phone to capture curriculum-based photographs or videos, provided

this is solely for legitimate educational purposes and all requirements of this Policy are followed.

Where staff use a personal mobile phone to capture curriculum-based photographs or videos during activities, this is permitted only where:

- there is a clear educational purpose;
- images are uploaded to the secure AS2Educate storage system before the end of the working day;
- all images are permanently deleted from the personal device immediately after successful upload;
- images are never retained on personal devices, personal cloud storage or personal accounts.

Staff must never:

- upload images to personal cloud storage;
- share images through personal messaging applications;
- retain copies of student images for personal use;
- post images of students on personal social media accounts.

Parents, carers and visitors must not photograph or record other children without permission.

Any misuse of images will be treated as a safeguarding matter and may result in disciplinary action.

Social Media and Online Professional Conduct

AS2Educate recognises that social media can provide valuable opportunities for communication, networking and professional development. However, online behaviour can have significant safeguarding, professional and reputational implications.

All staff are expected to maintain the same high standards of professional conduct online as they do within the workplace.

This section applies to:

- social networking sites;
- messaging applications;
- discussion forums;
- blogs;
- podcasts;
- online gaming platforms;
- video-sharing platforms;
- artificial intelligence platforms;
- any future digital communication technologies.

Examples include Facebook, Instagram, LinkedIn, X (formerly Twitter), TikTok, Snapchat, WhatsApp, Threads, Discord, YouTube and similar services.

Professional Boundaries

Staff must maintain clear professional boundaries at all times.

Staff must not:

- accept friend or follow requests from current students;
- initiate contact with students through personal social media accounts;
- communicate with students using personal messaging services;
- share personal contact details with students;
- access or monitor students' personal social media accounts unless there is a legitimate safeguarding reason authorised through safeguarding procedures.

Former students who remain under the age of 18 should continue to be treated as students for the purposes of this Policy.

Where safeguarding concerns arise through online activity, staff must follow the Safeguarding and Child Protection Policy rather than attempting to manage concerns themselves.

Professional Reputation

Staff should remember that information shared online may remain publicly accessible permanently, even where privacy settings are used.

Staff should:

- regularly review privacy settings;
- ensure online content reflects professional standards;
- consider whether posts could undermine confidence in their professional role;
- avoid engaging in online arguments that may affect the reputation of AS2Educate.

Where staff identify themselves as working for AS2Educate on professional networking sites such as LinkedIn, information must remain factual and professional.

If expressing personal opinions which may reasonably be associated with AS2Educate, staff should make clear they are speaking in a personal capacity and not on behalf of the organisation.

Confidentiality

Staff must never publish, disclose or discuss:

- safeguarding information;
- student information;
- confidential organisational information;
- information relating to colleagues;
- information about parents or families;
- photographs taken within the provision;
- information that could identify a child or family.

This applies even where names have been removed if individuals could still be identified.

Online Conduct

Staff must not use social media or online platforms to:

- criticise, undermine or bring AS2Educate into disrepute;
- bully, intimidate or harass others;
- make discriminatory or offensive comments;
- share confidential information;
- engage in unlawful activity;
- post material inconsistent with the Staff Code of Conduct.

Low-level concerns relating to online conduct should be reported in accordance with the Low-Level Concerns Policy to allow patterns of behaviour to be identified and addressed at an early stage.

Any online behaviour that may indicate a safeguarding concern must be reported immediately to the Designated Safeguarding Lead.

Monitoring and Compliance

AS2Educate reserves the right to monitor the use of its devices, networks, email systems and internet access in accordance with UK GDPR, the Data Protection Act 2018 and relevant employment legislation.

Monitoring will always be proportionate, lawful, transparent and carried out in accordance with UK GDPR and employment legislation:

- safeguarding children;
- protecting organisational systems;
- investigating security incidents;
- preventing misuse;
- ensuring compliance with organisational policies.

Any breach of this Policy may result in:

- additional training;
- informal management action;
- withdrawal of IT access;
- disciplinary action up to and including dismissal;
- referral to external agencies where appropriate.

Serious breaches involving safeguarding, criminal activity or data protection will be managed in accordance with the Safeguarding and Child Protection Policy, Staff Disciplinary Policy, Data Protection Policy and relevant statutory guidance.

Remote Learning and Online Meetings

Where remote learning or online meetings are used, AS2Educate will ensure that:

- only approved platforms are used;
- professional standards are maintained at all times;
- safeguarding procedures apply equally to online sessions;
- staff maintain appropriate professional boundaries;

- sessions are appropriately supervised and recorded where required;
- students are protected from inappropriate online contact.

Staff must never conduct online learning using personal social media or personal video conferencing accounts.

Reporting Online Safety Concerns

Students are encouraged to report anything online that:

- worries or upsets them;
- makes them feel unsafe;
- involves bullying, threats or coercion;
- requests personal information;
- involves inappropriate images or videos;
- appears illegal or harmful.

Staff must immediately report:

- safeguarding concerns arising online;
- making, sharing or threatening to share nudes or semi-nudes, image-based abuse, deepfakes or other AI-generated or digitally manipulated sexual imagery;
- concerning monitoring alerts;
- attempted access to harmful content;
- cyber security incidents;
- phishing attempts;
- suspected data breaches;
- misuse of artificial intelligence;
- cyberbullying;
- suspected online exploitation; and
- any online behaviour indicating a risk of harm.

Concerns will be managed in accordance with the Safeguarding and Child Protection Policy and may involve Children's Social Care, the Police, CEOP, the Local Authority Designated Officer (LADO), Prevent partners or other appropriate agencies.

Behaviour and Consequences

Where technology is misused, AS2Educate will adopt a proportionate and educational response wherever possible.

Responses may include:

- restorative conversations;
- additional online safety education;
- temporary restriction of device access;
- behaviour support strategies;
- parental involvement;
- safeguarding intervention;
- disciplinary action for staff;
- referral to external agencies where appropriate.

Where misuse indicates abuse, exploitation or criminal activity, safeguarding procedures will take precedence over behaviour sanctions.

Monitoring, Review and Continuous Improvement

The Provision Manager and Designated Safeguarding Lead are responsible for monitoring the implementation of this Policy.

This includes reviewing:

- filtering effectiveness;
- monitoring arrangements;
- safeguarding incidents involving technology;
- patterns and emerging online risks;
- staff compliance;
- training needs;
- technological developments;
- changes to statutory guidance.

Learning arising from incidents, audits or safeguarding reviews will be used to strengthen digital safeguarding, improve staff practice and enhance students' online safety.

This Policy will be reviewed annually, or sooner where there are changes to legislation, statutory guidance, technology or organisational practice.

Digital Safety, Acceptable Use and Professional Online Conduct Declaration

Reviewed by:	Richard Fihosy and Claire Ames
Policy Commencement Date:	17/07/2026
Ratified by:	Provision Manager and DSL
Review:	Annual
Next Review:	Autumn Term 2027
July 26	This Policy combines AS2Educate's previous Acceptable Use of IT Policy, E-Safety Policy and Social Networking Policy into one comprehensive framework governing the safe use of technology and professional online conduct. Full policy and compliance review