



IWYS Alternative Provision Online Safety Policy

Policy owner	IWYS Alternative Provision
Approved by	Proprietor – Charmaine Baines
Approval date	October 2026
Review date	October 2027

1. Policy statement

IWYS Alternative Provision (IWYS) recognises that digital technology supports learning, communication and access to services, but can expose children and young people to risks. We are committed to keeping learners safe online, promoting respectful and responsible digital behaviour, protecting personal information, and responding promptly to concerns.

This policy applies to all learners, employees, agency staff, volunteers, visitors, contractors and any other adults working on behalf of IWYS. It applies on site, during off-site activities, when working remotely, and whenever IWYS systems, devices, accounts or communications are used.

Online safety is part of safeguarding and behaviour management. It is not limited to filtering or monitoring technology. Staff must consider the individual needs, vulnerabilities, communication needs and circumstances of learners, including those who may have experienced exclusion, trauma, exploitation or disrupted education.

2. Aims

- Provide a clear, consistent approach to online safety across the provision.
- Help learners recognise online risks and make safer, informed choices.
- Set clear expectations for staff and learner use of devices, networks, platforms and social media.
- Reduce the risk of harmful or inappropriate content, contact and conduct.
- Protect personal, sensitive and confidential information.
- Ensure online safety concerns are reported, recorded, assessed and acted on promptly.
- Work with parents/carers, placing schools, local authorities and relevant agencies where appropriate.

3. Scope and definitions

Online safety includes the safe use of internet services, email, messaging, social media, gaming, video and livestreaming platforms, search engines, cloud services, learning platforms, mobile devices, artificial intelligence (AI) tools and other connected technologies.

The policy covers risks commonly grouped as:

- Content: exposure to harmful, illegal, misleading or age-inappropriate material.
- Contact: grooming, coercion, exploitation, scams, unwanted communication or contact from unsafe individuals.
- Conduct: cyberbullying, harassment, threats, hate, sharing images without consent, impersonation or harmful group behaviour.
- Commerce and data: fraud, phishing, in-app purchases, financial exploitation, identity theft and loss of personal data.

This policy should be read alongside IWYS's safeguarding and child protection policy, behaviour policy, staff code of conduct, acceptable use agreements, data protection/privacy arrangements, complaints procedure, health and safety policy, and relevant placing-school arrangements.

4. Roles and responsibilities

4.1 Proprietor / management committee

- Ensure online safety is treated as a safeguarding priority and that this policy is reviewed and implemented.
- Provide appropriate resources, staff training and oversight of filtering and monitoring arrangements.
- Review significant incidents and ensure lessons are learned.

4.2 Provision Lead

- Ensure staff, learners and parents/carers know the relevant rules and reporting routes.
- Ensure proportionate filtering and monitoring is in place, reviewed and tested, with risks and gaps recorded.

- Ensure incidents are escalated, recorded and addressed, including referrals to external agencies where required.
- Ensure staff induction and refresher training cover online safety, data protection and reporting procedures.

4.3 Designated safeguarding lead (DSL)

- Lead the safeguarding response to online safety concerns and consider whether a child protection referral is needed.
- Coordinate with the local authority, placing school, police, children's social care or other agencies as appropriate.
- Maintain confidential safeguarding records and ensure information is shared lawfully and proportionately.
- Keep up to date with current online harms, local procedures and relevant statutory guidance.

4.4 All staff, volunteers and contractors

- Model safe, respectful and professional online behaviour.
- Use only approved systems and follow this policy and the staff code of conduct.
- Report concerns immediately through the safeguarding route; do not promise secrecy.
- Protect passwords, devices, learner information and confidential communications.
- Never use personal accounts to communicate privately with learners or exchange inappropriate content.

4.5 Learners

- Use devices, accounts and the internet in line with the learner acceptable use agreement and staff instructions.
- Treat others respectfully and do not bully, threaten, impersonate, record or share content about others without permission.
- Keep passwords private and do not try to bypass safety settings or access another person's account.
- Tell a trusted adult if something online worries them, if someone asks for personal information or images, or if they see harmful content.
- Understand that unsafe or harmful online behaviour may lead to safeguarding action and proportionate consequences.

4.6 Parents and carers

Parents/carers are encouraged to discuss online experiences with their child, use suitable safety and privacy settings, and contact IWYS if they are concerned. IWYS will share advice and information where appropriate, taking account of safeguarding, confidentiality and the learner's circumstances.

5. Education and prevention

Online safety education will be age-appropriate, accessible and responsive to learners' abilities, experiences and needs. It may be delivered through tutorials, personal development, individual support, group work and curriculum activities.

- Recognising grooming, exploitation, coercion, scams, misinformation and unsafe requests.
- Privacy, personal information, passwords, multi-factor authentication and account security.
- Cyberbullying, respectful communication, consent, digital footprints and reporting harmful content.
- Image-sharing, intimate images, livestreaming, location sharing and the risks of meeting online contacts.
- Managing screen time, online wellbeing and seeking help when online activity becomes distressing.
- AI-generated content, deepfakes, impersonation, misinformation, plagiarism and safe use of AI tools.

Staff should revisit relevant topics after incidents or when new risks emerge. Learners should be given clear, non-judgemental routes to ask for help.

6. Acceptable use of devices and systems

6.1 IWYS equipment and network

- Learners may use IWYS devices and network only with permission and appropriate supervision.
- Users must not access, create, download, store or share illegal, abusive, hateful, sexually explicit or otherwise harmful content.
- Users must not bypass filters, install unauthorised software, connect unauthorised devices, interfere with security controls or attempt to access another user's files or account.
- Downloading, gaming, streaming, online shopping and use of removable media must follow staff instructions and local IT controls.
- Devices should be locked when unattended; suspected malware, lost devices or security weaknesses must be reported promptly.

6.2 Personal devices

IWYS will set clear rules for learner mobile phones, smartwatches, headphones and other personal devices. Unless an agreed adjustment or learning activity applies, devices should be kept away during teaching and support sessions and used only with staff permission. Staff must not routinely use personal devices to photograph, record or communicate with learners.

6.3 Remote learning and online meetings

- Use approved platforms and IWYS-managed accounts wherever possible.
- Use appropriate backgrounds, professional language and suitable clothing; protect meeting links and access codes.
- Staff should avoid one-to-one online sessions unless authorised, risk-assessed and conducted in line with safeguarding procedures.
- Do not record a session or take screenshots unless there is a clear, authorised purpose, appropriate notice and lawful handling of the recording.
- Parents/carers and learners should know how to report inappropriate contact or technical/safety concerns.

7. Staff communications, social media and professional boundaries

- Staff must use approved work accounts and channels for contact with learners and families.
- Staff must not add learners to personal social media accounts, use disappearing-message services for professional contact, or communicate through unauthorised private accounts.
- Staff must not share personal contact details with learners except where specifically authorised and risk-assessed.
- Staff must not publish images, names, locations, personal stories or other identifying information about learners without appropriate authorisation and a lawful basis.
- Staff must not post comments or images online that could compromise professional boundaries, confidentiality, safeguarding or public confidence in IWYS.
- Any accidental or inappropriate contact must be reported to the Provision Lead/DSL promptly and recorded.

8. Filtering, monitoring and technical security

IWYS will take proportionate steps to prevent access to harmful or inappropriate material and to identify possible misuse. The Provision Lead will document the systems used, who reviews alerts, how concerns are escalated and how effectiveness is checked. Where IT is managed by a host, provider or placing school, responsibilities and escalation routes must be agreed in writing.

- Use age-appropriate filtering and security settings on IWYS-managed networks and devices.
- Apply software updates, anti-malware protection, access controls and secure configuration where applicable.

- Restrict administrative privileges and promptly remove access when staff or contractors leave or change roles.
- Review filtering and monitoring arrangements at least annually and after a significant incident, system change or identified gap.
- Explain monitoring to staff and learners in clear terms; monitoring must be lawful, necessary, proportionate and consistent with privacy and data protection requirements.
- Do not rely on filtering alone: staff supervision, education and clear reporting routes remain essential.

Local arrangements to complete: filtering/monitoring provider: [insert]; person who reviews alerts: [insert]; out-of-hours escalation route: [insert]; IT support contact: [insert].

9. Data protection, privacy and information security

- Personal data must be collected, accessed, used, stored, shared and deleted only for authorised purposes and in line with IWYS data protection arrangements.
- Use approved storage and sharing systems; do not send learner data to personal email accounts or unauthorised cloud services.
- Share information only with people who need it for a legitimate purpose, using secure methods.
- Use strong, unique passwords and multi-factor authentication where available. Never share passwords or authentication codes.
- Check recipients and attachments before sending messages; use appropriate protections for sensitive information.
- Report suspected data breaches, phishing, account compromise, misdirected emails or lost devices immediately to the Provision Lead and data protection lead.
- Do not upload identifiable learner information, safeguarding records, photographs or confidential work to public AI tools unless the tool and use have been expressly approved and lawful safeguards are in place.

The data protection lead / Data Protection Officer (if appointed) is: [insert name and contact details].

10. Artificial intelligence and emerging technologies

AI tools may be used only where approved by IWYS and for an appropriate educational or operational purpose. Staff remain responsible for checking outputs for accuracy, bias, age-appropriateness and safeguarding risks. Confidential or personal information must not be entered into public AI tools without explicit approval and appropriate safeguards.

- Do not use AI to create, alter or distribute sexualised, humiliating, threatening or deceptive images or content about a learner or colleague.
- Treat AI-generated content, links, images, voices and messages critically; they may be false or manipulated.
- Learners must follow staff instructions about permitted AI use and must not use it to bully, impersonate, deceive or bypass safety controls.
- Concerns about deepfakes, impersonation or AI-enabled exploitation must be reported and handled as safeguarding concerns.

11. Responding to online safety incidents

All concerns must be taken seriously. Staff should respond calmly, avoid blaming the learner, preserve relevant information where safe to do so, and notify the DSL or Provision Lead without delay.

11.1 Immediate response

1. If a child or another person is in immediate danger, contact emergency services and follow safeguarding procedures.
2. Listen to the learner, reassure them that they have done the right thing by telling someone, and do not promise confidentiality.

3. Record the concern factually, including dates, times, people involved, what was reported and any action taken.
4. Report the concern to the DSL promptly. If the DSL is implicated or unavailable, use the alternative safeguarding route: [insert name/role and contact].
5. Do not investigate beyond your role, confront an alleged perpetrator, forward harmful content, or ask a learner to resend an image.
6. Preserve URLs, usernames, dates and relevant messages where safe and lawful. Do not download or circulate illegal or sexual images of children.
7. The DSL will assess risk, decide on referrals and coordinate with parents/carers, placing schools and agencies where appropriate and safe.

11.2 Examples of incidents requiring action

- Cyberbullying, threats, harassment, hate incidents or discriminatory content.
- Grooming, sexual exploitation, coercion, blackmail, requests for intimate images or suspicious adult contact.
- Sharing or threatened sharing of intimate images, including AI-generated sexual images.
- Exposure to self-harm, suicide, extremist, violent or other harmful content.
- Sextortion, scams, fraud, identity theft, account compromise or unauthorised access.
- Disclosure or loss of personal data, inappropriate staff contact, or bypassing safety controls.

The DSL should follow current statutory guidance and local safeguarding partnership procedures, including referral to children's social care, police or specialist services where appropriate. Where a concern relates to a staff member, the allegation management procedure and the Local Authority Designated Officer (LADO) process should be considered as applicable.

12. Bullying, harmful behaviour and consequences

Online behaviour that harms, intimidates or humiliates others will be addressed under the behaviour and safeguarding policies. Responses should be proportionate, consistent, restorative where appropriate, and sensitive to disability, additional needs, communication needs and the context of the incident. Safeguarding action may be required regardless of whether a behaviour policy consequence is applied.

Possible responses include education, restorative work, contact with parents/carers or placing schools, restriction of device or account access, a risk assessment, a safeguarding referral or disciplinary action. Serious or potentially criminal behaviour will be escalated to the relevant agencies.

13. Filtering out harmful content and managing prohibited material

If a user encounters harmful or illegal material, they should stop viewing it and report it to a member of staff. Staff should not search for, copy, save or distribute illegal material. If prohibited content is found on a device, do not continue exploring the device; secure it where safe to do so and seek advice from the DSL/Provision Lead and appropriate authorities. Any action must preserve evidence and protect the child.

14. Visitors, contractors and third-party providers

Visitors and contractors must follow IWYS instructions on device use, photography, recording, network access and confidentiality. Access to systems must be limited to what is necessary and authorised. Contracts or service agreements with IT providers and online platforms should clarify security, filtering/monitoring, data protection, incident notification and support responsibilities.

15. Training, communication and review

- All staff will receive online safety and safeguarding guidance at induction and regular refresher training.
- Learners will receive the policy in an accessible format and will be supported to understand the rules.
- Parents/carers and placing schools will be informed of relevant expectations and reporting routes.

- The Provision Lead and DSL will monitor incidents, training needs, technology changes and emerging risks.
- This policy will be reviewed at least annually and sooner following significant incidents, changes in law/guidance, a change of provider or changes to IWYS's operating model.

16. Related policies and guidance

Read this policy alongside the current versions of:

- IWYS Safeguarding and Child Protection Policy.
- IWYS Behaviour Policy and Staff Code of Conduct.
- IWYS Data Protection / Privacy Policy and breach reporting procedure.
- IWYS Acceptable Use Agreement for staff and learners.
- Current Department for Education safeguarding and filtering/monitoring guidance.
- Keeping Children Safe in Education (current edition).
- Working Together to Safeguard Children (current edition).
- Relevant local safeguarding partnership procedures and placing-school requirements.

Appendix A — Learner online safety agreement

I will:

- Use devices, accounts and websites only as staff allow.
- Be respectful online and not bully, threaten, discriminate against or impersonate anyone.
- Keep passwords private and protect my personal information.
- Not take or share photos, videos, screenshots or personal information about others without permission.
- Not try to access harmful content, bypass filters or use someone else's account.
- Tell a trusted adult if something online worries me or someone asks me to do something unsafe.
- Follow staff instructions and understand that unsafe use may lead to support, safeguarding action or proportionate consequences.

Learner name: _____ Signature: _____

Date: _____ Staff witness: _____

Appendix B — Staff online safety checklist

- ☐ I have read and understood this policy and the staff code of conduct.
- ☐ I use approved accounts and platforms for professional communication.
- ☐ I maintain appropriate boundaries and do not contact learners through personal accounts.
- ☐ I protect learner data and report suspected breaches immediately.
- ☐ I know who the DSL is, how to report concerns and what to do if the DSL is implicated.
- ☐ I know how to report harmful content, inappropriate contact and technical security incidents.
- ☐ I understand the rules for AI tools, recording, photography and remote sessions.

Staff name: _____ Signature: _____

Date: _____

Appendix C — Incident record prompt

- Date/time concern received and by whom.
- Name(s) of learner(s) and others involved, with relevant context.
- What was seen, heard or reported (record exact words where useful; distinguish fact from opinion).
- Platform/device/account and any available URL, username or relevant timestamps.
- Immediate safety actions taken and who was informed, with times.
- Whether evidence was preserved safely and lawfully; do not attach or circulate illegal imagery.
- DSL risk assessment, decisions, referrals, parent/carers or placing-school contact and rationale.
- Follow-up actions, responsible person and review date.

Appendix D — Approval and review record

Version	Date	Changes made	Approved by
[Complete]	[Complete]	[Complete]	[Complete]
[Complete]	[Complete]	[Complete]	[Complete]
[Complete]	[Complete]	[Complete]	[Complete]