



IWYS

Alternative Provision

Acceptable Internet

and ICT Use Policy

Policy owner	Head of Provision / Designated Safeguarding Lead (DSL)
Approved by	Charmaine Baines
Date approved	Oct 2026
Review date	Oct 2027 - or after significant incidents or changes
Applies to	Staff, learners, volunteers, contractors, visitors and other authorised users

1. Purpose and principles

IWYS Alternative Provision provides access to internet services and information and communication technology (ICT) to support education, communication, administration and safe participation in learning. This policy sets out the standards expected of everyone using IWYS systems or accessing digital services for IWYS activities.

- Protect learners and adults from online harm, exploitation, abuse, inappropriate content and cyber security threats.
- Support purposeful learning, digital skills, inclusion and responsible online behaviour.
- Protect personal information, confidential records, devices, accounts and the reputation of IWYS.
- Make clear that online behaviour is subject to the same expectations of safety, dignity and respect as face-to-face behaviour.
- Use filtering and monitoring as safeguards alongside supervision, education and professional judgement—not as a replacement for them.

2. Scope

This policy applies to IWYS-owned, managed or supplied devices, networks, Wi-Fi, email, accounts, cloud services, learning platforms, messaging and collaboration tools, software and data. It applies on site, during off-site activities and during remote learning where users access IWYS systems or act on behalf of IWYS.

Personal devices used for learning or connected to IWYS networks must follow the relevant parts of this policy and any separate bring-your-own-device rules. IWYS cannot guarantee control over activity on private devices, networks or third-party platforms outside its management; concerns should still be reported.

3. Core rules for all users

- Use ICT primarily for authorised educational, safeguarding, administrative or other approved purposes.
- Treat others respectfully. Do not bully, harass, threaten, discriminate against, impersonate or deliberately humiliate anyone online.
- Access only accounts, files, systems and information you are authorised to use.
- Keep passwords, passcodes and authentication codes private. Use approved multi-factor authentication where required.
- Lock or sign out of devices when not in use; never leave a logged-in device accessible to others.
- Follow copyright, licensing, privacy, confidentiality and data protection requirements.
- Do not attempt to bypass filtering, monitoring, security controls or access restrictions.
- Report suspicious messages, unsafe content, accidental disclosures, lost devices, security warnings and other concerns promptly.
- Follow staff instructions and any additional rules for a particular device, lesson, activity or service.

4. Prohibited use

Users must not use IWYS systems or devices to:

- View, create, store, download, upload or share illegal, abusive, exploitative, sexually explicit or otherwise seriously harmful material.
- Search for, possess, create or share child sexual abuse material, or share intimate images without consent. Do not copy, forward or investigate suspected illegal images; report them immediately and follow safeguarding instructions.
- Promote terrorism, violent extremism, self-harm, suicide, hate or serious violence, or encourage others to engage in harmful or illegal acts.

- Engage in cyberbullying, stalking, doxxing, discriminatory abuse, threats, unwanted sexual communication or malicious impersonation.
- Access gambling, pornography, weapons-related, malware, phishing or other restricted services except where a specific, lawful and authorised educational or professional purpose has been risk-assessed and approved.
- Install unauthorised software, apps, browser extensions, VPNs, proxies or remote-access tools, or disable security settings.
- Attempt to gain unauthorised access, scan or attack systems, spread malware, guess passwords, interfere with networks or disrupt services.
- Use another person's account, share credentials, falsify records or conceal activity by deleting or altering logs.
- Share confidential or personal information without authorisation, including learner records, safeguarding information, addresses, contact details, passwords or identifiable photographs.
- Record, photograph, livestream or audio-record learners, staff or visitors without appropriate authorisation and consent/legal basis.
- Use ICT to commit fraud, infringe copyright, make unauthorised purchases or conduct personal business that interferes with work or learning.
- Use generative AI or other automated tools to create harmful content, impersonate others, submit dishonest work, disclose confidential information or make decisions about learners without authorisation.

5. Learner expectations

Learners are expected to use devices for the task set, follow staff instructions, keep login details secure, respect other people's privacy, and report content or contact that makes them feel unsafe. Learners must not use devices to distract others, access restricted content, take or share images without permission, or contact other learners in ways that are threatening, abusive or inappropriate.

Staff should explain rules in language and formats appropriate to each learner's age, understanding, communication needs and vulnerabilities. Individual risk assessments and reasonable adjustments may be needed but must not remove essential safeguarding protections without documented consideration and approval.

6. Staff and adult user expectations

- Use professional judgement and maintain appropriate professional boundaries in all digital communications with learners and families.
- Use approved accounts, platforms and channels for work with learners. Do not use personal social-media accounts or private messaging to communicate with learners unless an explicit, documented exception has been authorised under safeguarding procedures.
- Do not exchange personal contact details or arrange private online contact with learners outside authorised arrangements.
- Keep learner and safeguarding information confidential and share it only with authorised recipients who need it.
- Do not access learner accounts or records out of curiosity or use monitoring data for personal reasons.
- Use only approved methods to store, transfer, print or dispose of sensitive information.
- Report concerns about a colleague's digital conduct through the safeguarding, low-level concerns, whistleblowing or other relevant procedure.

7. Email, messaging and online communication

- Check recipients carefully before sending messages or attachments, especially where personal or safeguarding data is involved.
- Do not open suspicious links or attachments, respond to unexpected requests for passwords or payments, or approve unexpected authentication prompts.
- Use approved work email and communication systems for official business and retain records in line with IWYS procedures.
- Do not send abusive, discriminatory, threatening or sexually inappropriate messages, or forward harmful content.
- Report phishing, suspected scams, mistaken recipients and accidental disclosures promptly.

8. Personal data, photos and recordings

Personal data must be collected, accessed, used and shared only for an authorised purpose and in accordance with IWYS privacy information and data protection procedures. Store information only in approved locations, use secure transfer methods, and apply access restrictions. Do not save learner records to personal email, unapproved cloud storage, removable media or consumer apps.

Photographs, video, audio and livestreaming involving learners require an authorised purpose and appropriate permissions or other lawful basis, with safeguarding and privacy considerations addressed. Consent alone may not be sufficient in every context. Never share images or details that could identify or locate a learner on personal accounts or public platforms unless explicitly authorised under IWYS procedures.

9. Internet filtering and monitoring

Use of IWYS networks, devices and accounts may be subject to filtering, security logging, monitoring and review in line with the Filtering and Monitoring Policy and applicable law. Monitoring may identify blocked access attempts, suspicious activity, security events or potential safeguarding concerns. Users should not assume that activity on IWYS systems is private.

Monitoring must be proportionate, transparent and restricted to authorised purposes. Alerts may be inaccurate or incomplete and will be assessed in context. Concerns are escalated to the DSL or relevant senior leader under the established procedures. The exact scope of monitoring depends on the systems and services in use.

10. Artificial intelligence and online tools

- Use only AI tools and online services approved for the intended purpose.
- Never enter identifiable learner information, safeguarding details, confidential documents, passwords or other sensitive data into a public AI tool unless specifically approved under IWYS data protection and security arrangements.
- Check AI-generated information for accuracy, bias, appropriateness and copyright concerns; do not treat it as a substitute for professional judgement.
- Staff must not use AI alone to make safeguarding, disciplinary, placement or other significant decisions about a learner.
- Learners must follow staff instructions about permitted AI use and be honest about when and how it has been used.

11. Devices, software and cyber security

- Use approved, supported devices and software; do not make unauthorised changes to device settings or security controls.
- Install updates and security patches as directed and restart devices when required.
- Do not connect unknown USB drives or other removable media. Follow IT instructions before using removable storage.
- Store devices securely and report loss, theft, damage or suspected compromise immediately.
- Do not connect unauthorised equipment to IWYS networks or share network access with unauthorised people.
- Use secure connections and approved remote-access methods; avoid accessing sensitive work over public Wi-Fi unless authorised safeguards are in place.

12. Reporting concerns and incidents

Report concerns promptly, even if you are unsure whether a breach has occurred. Do not delay reporting while trying to investigate or collect proof.

- Safeguarding concern, harmful contact or concerning content: report immediately to the DSL/deputy DSL using the safeguarding procedure.
- Immediate danger or urgent risk of serious harm: follow emergency procedures and contact emergency services where appropriate.
- Cyber security issue, phishing, malware, lost device or unauthorised access: contact the designated IT/security lead and senior leader; involve the DSL where learner safety may be affected.
- Personal data breach or information sent to the wrong person: notify the designated data protection lead promptly and follow the data breach procedure.
- Concern about staff conduct: use the safeguarding, low-level concerns, whistleblowing or complaints procedure as appropriate.

Preserve relevant messages and records where safe and lawful, but do not forward or copy suspected illegal imagery or content. Follow instructions from the DSL, IT/security lead or relevant authorities.

13. Breaches and consequences

A breach may lead to proportionate action based on the nature, seriousness, context, age and needs of the user, and any safeguarding implications. Possible responses include education and support, parental/carers involvement, a risk assessment, restriction or suspension of access, behaviour or disciplinary action, referral to safeguarding agencies or police, and action under employment or contractual procedures. Serious concerns may require immediate protective action.

No user should be discouraged from reporting a concern in good faith. Reports will be handled sensitively and fairly, with confidentiality maintained as far as possible and consistent with safeguarding duties.

14. Training, review and communication

Users will be made aware of the rules relevant to them. Staff and contractors will receive induction and periodic updates on online safety, data protection, cyber security and reporting routes. Learners will receive age- and needs-appropriate guidance and will be asked to confirm that they understand the learner rules. This policy will be reviewed at least annually and after significant incidents, changes to systems or relevant guidance.

15. Related policies and guidance

- Safeguarding / Child Protection Policy
- Online Safety Policy
- Filtering and Monitoring Policy
- Behaviour and Anti-Bullying Policies
- Data Protection, Privacy and Records Retention Policies
- Cyber Security / Incident Response Procedure
- Staff Code of Conduct and Whistleblowing Policy
- Current Keeping Children Safe in Education and Department for Education filtering and monitoring standards

Appendix A — Learner Acceptable Use Agreement

I agree to use IWYS internet, devices and accounts safely and respectfully. I will:

- ☐ Use technology for the learning or activity I have been asked to do.
- ☐ Follow staff instructions and not try to get around filtering or security.
- ☐ Keep my password private and use only my own account.
- ☐ Treat others respectfully and not bully, threaten or embarrass anyone online.
- ☐ Not look for, create or share harmful or inappropriate content.
- ☐ Ask before taking or sharing photographs, recordings or personal information.
- ☐ Tell a trusted member of staff if something online worries me or if I make a mistake.

Learner name: _____ Date: _____

Learner signature (where appropriate): _____

Staff member: _____ Parent/carer (if applicable): _____

Appendix B — Staff / adult user declaration

I have read or been briefed on this policy and agree to follow it, protect confidential information, use approved systems, maintain professional boundaries, and report concerns promptly.

Name: _____ Role: _____

Signature: _____ Date: _____

Approval and review record

Approved by: _____ Role: _____

Signature: _____ Date: _____

Next review due: _____