



IWYS Alternative Provision Filtering and Monitoring Policy

Policy owner	Designated Safeguarding Lead (DSL) / Head of Provision
Approved by	Charmaine Baines
Date approved	Oct 2026
Review date	Oct 2027 after a significant incident or system change]
Applies to	All staff, learners, contractors, visitors and anyone using IWYS systems or networks

1. Purpose and principles

IWYS Alternative Provision is committed to safeguarding learners and staff when they use the internet, digital devices, online services and communication platforms. Filtering and monitoring are complementary safeguards: filtering aims to prevent access to harmful or inappropriate content, while monitoring helps identify possible unsafe activity, safeguarding concerns and misuse.

Controls will be proportionate to learners' ages, needs and vulnerabilities, the risks associated with alternative provision, and the systems being used. They will support safe education rather than replace supervision, professional judgement, teaching about online safety or the provision's safeguarding procedures.

- Safeguarding is the priority; concerns must be acted on, not simply recorded by a system.
- Controls should be effective, age-appropriate, regularly tested and no more restrictive than necessary for safe learning.
- Staff must not assume that filtering or monitoring will identify every risk.
- Learners will be told in accessible language what is monitored, why, and how to seek help.
- Personal data and monitoring records will be accessed only by authorised people for legitimate purposes.

2. Scope

This policy applies to IWYS-owned, managed or provided devices, networks, Wi-Fi, accounts, browsers, cloud services, learning platforms and other digital services used for provision business or learning. It also applies to personal devices when they connect to IWYS networks or are used in supervised learning, to the extent permitted by law and the relevant acceptable-use arrangements.

It covers on-site and remote learning where IWYS has control over the relevant account, device, service or connection. IWYS cannot guarantee visibility of activity on unmanaged personal devices, private networks or third-party services outside its control. Staff should report concerns even where the activity cannot be technically verified.

3. Roles and responsibilities

Role	Responsibilities
Proprietor	Ensure suitable systems, resources, oversight and review are in place; approve this policy and receive assurance about effectiveness and incidents.
Head of Provision / senior leader	Ensure the policy is implemented, staff understand their duties, actions are followed up, and risks are addressed.
Designated Safeguarding Lead (DSL)	Lead safeguarding decisions arising from alerts or reports; assess risk, keep safeguarding records, refer to children's social care/police where appropriate, and liaise with the filtering/monitoring lead.
Filtering and monitoring lead / IT provider	Maintain an accurate record of systems and responsibilities; configure, test and review controls; investigate technical issues; preserve relevant logs; and report significant failures promptly.
All staff and contractors	Follow acceptable-use and safeguarding procedures, supervise learners appropriately, report concerns immediately, and never bypass or disable controls without authorisation.
Learners	Use systems safely and respectfully, follow the learner acceptable-use agreement, and tell a trusted adult if they encounter disturbing content, receive unsafe contact or believe a control is not working.
Parents/carers	Support safe use and raise concerns with IWYS; receive appropriate information about online safety and the provision's approach.

4. Filtering arrangements

IWYS will use an appropriately configured filtering solution for internet access under its control. The provision will document the product/service, who manages it, which devices and users it covers, and how settings are applied. The following controls should be configured where supported and appropriate:

- Block known illegal content and high-risk categories, including child sexual abuse material, extremist/terrorist content, and content promoting self-harm or serious harm.
- Restrict age-inappropriate sexual content, pornography, gambling, violence, hate, weapons, malware, phishing and other harmful categories.
- Apply safe-search and restricted-mode settings to search engines, video platforms and other services where available.
- Use user/group profiles where appropriate, while maintaining a consistent safeguarding baseline.
- Control installation of unauthorised apps, browser extensions, VPNs, proxies and other tools that could bypass safeguards.
- Review allow-lists and exceptions so they are limited, documented, time-bound where possible and approved by an authorised person.
- Ensure filtering remains active on managed devices and remote access arrangements where IWYS is responsible for the connection or endpoint.

Filtering must not be treated as infallible. Staff should report blocked or accessible content that appears wrongly categorised. Any exception must have a clear educational or operational reason, a risk assessment where needed, approval by the Head of Provision or delegated lead, and a review date. Staff must not create informal workarounds.

5. Monitoring arrangements

IWYS will monitor digital activity proportionately to help identify safeguarding risks, policy breaches, cyber security threats and technical failures. The exact capability depends on the systems in use; the provision must accurately record what is monitored and must not claim visibility it does not have.

- Web requests, blocked attempts and security events recorded by the filtering service.
- Alerts for potentially harmful searches, repeated attempts to reach restricted content or other high-risk activity, where the product supports this.
- Security logs for managed devices, user accounts, email, collaboration tools and learning platforms, where available and appropriate.
- Reports from staff, learners, parents/carers, IT providers or other agencies.
- Periodic checks of configuration, coverage, alert routing and whether monitoring is functioning as intended.

Monitoring may generate false positives or miss harmful activity. Alerts must be assessed in context and must not, on their own, be treated as proof of misconduct. Monitoring is not a substitute for direct supervision, professional curiosity or a conversation with a learner when this is safe and appropriate.

6. Alert review and safeguarding response

The following response pathway applies to alerts or reports that may indicate a safeguarding concern:

1. Triage promptly: the designated monitoring reviewer checks the alert, available context, user/device details and whether the event is credible or urgent.
2. Escalate safeguarding concerns immediately to the DSL or deputy DSL. If a child may be at immediate risk of harm, follow emergency safeguarding procedures and contact emergency services/police as appropriate.
3. The DSL assesses the concern under the safeguarding/child protection policy, decides on protective action and referrals, and records the rationale and outcome securely.
4. Preserve relevant evidence and logs. Do not forward, download, copy or share illegal or potentially illegal images or content. Follow police/child-protection advice and internal procedures.

5. For cyber security incidents, unauthorised access or suspected compromise, notify the designated IT/security contact and senior leader as well as the DSL where safeguarding may be involved.
6. Record actions taken, the person responsible, timings, referrals and follow-up. Close the alert only when the outcome and any outstanding actions are documented.

Staff must not investigate a serious safeguarding concern beyond their role, promise confidentiality, confront a suspected perpetrator in a way that could increase risk, or delay escalation while trying to gather more evidence.

7. Learner support, education and accessibility

Learners will receive age- and needs-appropriate guidance about online safety, harmful content, online relationships, privacy, cyberbullying, exploitation, misinformation and how to report a concern. Staff should explain blocked pages calmly and use them as a learning opportunity where appropriate. Reasonable adjustments and individual risk plans may be needed for learners with SEND, trauma histories or specific vulnerabilities; these must not remove essential safeguarding protections without a documented risk assessment and authorised approval.

8. Privacy, data protection and records

IWYS will be transparent about monitoring and handle logs and alerts in accordance with UK data protection law, its privacy information, records-management arrangements and applicable employment requirements. Only authorised personnel may access monitoring records, and only for a defined safeguarding, security, compliance or operational purpose.

- Document the purpose and lawful basis for processing and provide clear privacy information to staff and learners, with parent/carer information where appropriate.
- Restrict access by role, use secure storage and transfer, and maintain an audit trail of access to sensitive records where feasible.
- Set and document retention periods based on purpose, safeguarding requirements, legal obligations and the data-protection retention schedule; securely delete records when no longer required.
- Share records only with people or agencies who need them, using approved secure channels and recording significant disclosures.
- Seek advice from the data protection lead / Data Protection Officer where applicable, especially for new monitoring technology, intrusive monitoring or a potential data protection impact assessment.
- Handle suspected personal data breaches under the data breach procedure and assess whether notification to the ICO or affected people is required.

9. Testing, review and assurance

The filtering and monitoring lead, with senior leadership and the DSL, will maintain a documented review cycle. As a minimum:

- Check filtering and monitoring coverage at induction of new devices/services and after material system or network changes.
- Test representative blocked categories, safe-search settings, alert generation and escalation routes at least termly, and after significant changes.
- Review logs, incidents, near misses, false positives, bypass attempts and user feedback at least termly.
- Review policy, roles, system settings and supplier arrangements at least annually and after a serious incident, safeguarding review or significant change.
- Record the date, tests performed, results, issues, remedial action, owner and completion date.
- Obtain assurance from any external IT or monitoring provider about system coverage, alerting, support arrangements and incident notification.

10. Failure, bypass or outage

Any suspected failure of filtering or monitoring, loss of logs, alert-routing failure or attempt to bypass controls must be reported promptly to the filtering/monitoring lead and senior leader. If safeguarding protection is materially reduced, the Head of Provision and DSL will assess immediate risk and introduce proportionate temporary measures, such as closer supervision, restricted access or pausing use of an affected service, until the issue is resolved. The incident and remediation must be recorded.

11. Training and communication

Staff and relevant contractors will receive induction and periodic updates on this policy, acceptable use, recognising online harm, alert handling, evidence preservation and escalation routes. Learners will be given an accessible acceptable-use agreement and shown how to report concerns. Parents/carers will be informed about the provision's approach and how to raise a concern.

12. Related documents

- Safeguarding / Child Protection Policy
- Online Safety Policy
- Staff and Learner Acceptable Use Agreements
- Behaviour Policy and Anti-Bullying Policy
- Data Protection, Privacy and Records Retention Policies

13. Legal and guidance framework

This policy should be read alongside current statutory guidance and applicable law, including Keeping Children Safe in Education (current edition), the Department for Education's filtering and monitoring standards for schools and colleges, Working Together to Safeguard Children (current edition), the UK GDPR and Data Protection Act 2018, and relevant safeguarding, equality and health and safety duties. IWYS must check the current versions before formal approval and adapt this policy to its registration status, commissioning arrangements and local safeguarding partnership procedures.

Appendix A — local systems and contacts (complete before approval)

Item	Local detail to complete	Owner / review
Filtering product/provider	[Name, service, support contact]	[Name / date]
Monitoring product/provider	[Name, service, support contact]	[Name / date]
Devices/accounts covered	[Managed devices, BYOD, remote learning scope]	[Name / date]
DSL / deputy DSL	[Names and secure contact details]	[Name / date]
Filtering & monitoring lead	[Name and contact details]	[Name / date]
IT/security escalation	[Name/provider and out-of-hours route]	[Name / date]
Data protection lead / DPO	[Name/contact or confirm not applicable]	[Name / date]
Log retention schedule	[Periods by log type and rationale]	[Name / date]
Safeguarding escalation route	[Local procedures, children's social care, police]	[Name / date]
Test record location	[Secure location and responsible person]	[Name / date]

Appendix B — Review and Test Log

Date	Test / review	Result / issue	Action owner & due date	Closed / evidence
[Complete]	[Complete]	[Complete]	[Complete]	[Complete]
[Complete]	[Complete]	[Complete]	[Complete]	[Complete]
[Complete]	[Complete]	[Complete]	[Complete]	[Complete]
[Complete]	[Complete]	[Complete]	[Complete]	[Complete]
[Complete]	[Complete]	[Complete]	[Complete]	[Complete]

Approval

Approved by: _____ Role: _____

Signature: _____ Date: _____

Next review due: _____