Nant Celyn Primary School
Online Safety Policy

With appendices - Updated August 2026

Table of Contents

Online Safety Policy Templates 3

- Introduction 3
- Purpose of the templates 3
- Expectations and statutory context 3
- Using the templates 4
- Scope of the Online Safety Policy 7
- Policy development, monitoring and review 7
- Schedule for approval, monitoring and review 7

Policy and leadership 8

- Responsibilities 8
- Online Safety Group 11

Policy 13

- Online Safety Policy 13
- Acceptable use 13
- Reporting and responding 18
- Responding to Learner Actions 22
- Responding to Staff Actions 24
- Use of Artificial Intelligence (AI) 25
- Online Safety Education Programme 27
- Staff 28
- Governors 29
- External Stakeholders 30
- Working with Parents and Carers 30
- Wider Community and Agencies 31

Technology 32

- Filtering and Online Safeguarding 32
- Technical Security 33
- Cyber Security 33
- Data Protection 34

Technology Practice 34

- Device Management 35
- Digital Content 35
- Public Online Communications 36

Outcomes 37

List of appendices 37

Appendix A1 - Learner Acceptable Use Agreement Template – for older learners 39

Appendix A2 - Acceptable Use Agreement Template – for Primary Learners 42
Appendix A3 - Acceptable Use Agreement Template – for younger learners 45
Appendix A4 - Parent/Carer Acceptable Use Agreement Template 46
Appendix A5 - Staff (and Volunteer) Acceptable Use Agreement Template 53
Appendix A6 - Acceptable Use Agreement for Community Users Template 57
Appendix A7 - Online Safety Policy Statement 59
Appendix A8 - Harmful Sexual Behaviour Policy Template (New) 62
Appendix A9 – Computer Misuse and Cyber Choices Policy Template 65
Appendix A10 - Responding to incidents of misuse – flow chart 68
Appendix A11 - Record of reviewing devices/sites (responding to incidents) 69
Appendix A12 - Reporting Log 70
Appendix B1 - Training Needs Audit Log 71
Appendix C1 – Web Filtering and Online Safeguarding Policy Template 72
Appendix C2 - Technical Security Policy Template 75
Appendix C3 - Cyber Security Policy Template 77
Appendix C4 - Data Security Policy Template 79
Appendix C5 – Public Online Communications Policy Template 84
Appendix C6 - Generative Artificial Intelligence (gen AI) in Schools 88
Legislation 105
Links to other organisations or documents 112

Online Safety Policy Templates

Introduction

These Online Safety Policy templates were updated and published in August 2026. They have been completely rewritten and are now more focussed, with more accessible language and reduced in length. Schools are recommended to customise this new policy to their own needs, rather than trying to edit the previous version.

Purpose of the templates

These policy templates are designed to support school leaders and governing bodies to produce an Online Safety Policy that is fit for purpose, proportionate, and grounded in a whole-school approach. The templates are intended to sit alongside, and align with, key policies including Safeguarding, Behaviour, and Anti-Bullying.

Online safety is part of a school's wider duty of care. Through an effective Online Safety Policy, schools meet statutory obligations to safeguard learners from harm within and outside school and strengthen the school's position in relation to accountability and legal challenge arising from the use of digital technology.

The templates set out the policy statements that the Welsh Government considers essential for good practice, alongside optional statements that schools may adopt to reflect their context and need.

Expectations and statutory context

An effective Online Safety Policy must be tailored to the needs of each school. Consultation and discussion with staff, learners, governors and, where appropriate, parents/carers, is a vital part of writing or reviewing the policy.

Schools should review their Online Safety Policy at least annually, and more frequently where there are significant changes in technology, risks, or technology-related behaviours.

Schools are subject to an increased level of scrutiny of their online safety practices by Estyn Inspectors during inspections, while the Counter Terrorism and Securities Act 2015 requires schools to ensure that children and young people are safe from terrorist and extremist material on the internet.

Keeping Learners Safe (April 2022) states:

> 7.16 The ability of educational establishments to recognise, respond to and resolve online safety issues should be verified by inspections from Estyn and the local authority.

Enhancing digital resilience in education: An action plan to protect children and young people online (November 2022) states:

> We, the Welsh Government, on behalf of Welsh Ministers, aim to help protect children and young people from illegal, harmful and false content on the internet and to promote safe, responsible and considerate behaviour online.
>
> With so many aspects of our lives now entwined with using technology in an online world, supporting our children and young people to be digitally resilient is fundamental.
>
> Keeping children and young people safe online is of critical importance and firmly a safeguarding matter in the twenty first century. We are committed to nurturing and promoting the safe and positive use of technology to children and young people by building a strong architecture around the child where professionals are skilled and families are aware of how to support children in their online lives. We seek to foster a protective environment for our children and young people by supporting families, practitioners, governors and other professionals creating a culture where keeping children safe online is everyone's business.
>
> The Curriculum for Wales aims to provide all our learners with high-level digital skills, to ensure our young people are digitally competent and resilient and evolve into enterprising, creative and critical thinkers.

With its optional statements and guidance notes, this portfolio of templates is longer than the resulting policy document is likely to be. It is intended that, while covering this complex and ever-changing issue, the resulting policy document should be concise and easily understood if it is to be effective and adopted by all. The templates are based on current best practice policies and procedures and schools can amend them to suit their requirements.

Using the templates

With optional statements and guidance notes, this portfolio is longer than the policy a school will typically publish. It is designed to help schools address a complex and fast-changing area while producing a final policy that is concise, accessible, and widely understood.

The first part of the document provides the main Online Safety Policy Template. Appendices include further and more detailed policy templates e.g., Acceptable Use Agreements. Schools can select, adapt and adopt the sections that best meet their needs.

Nant Celyn Primary Online Safety Policy

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Version: [?}

Date created: [18/09/26]

Next review date: [18/09/27]

Scope of the Online Safety Policy

This Online Safety Policy sets out how Nant Celyn Primary will safeguard members of our community online, in line with statutory guidance and best practice. The school is aware of the wider statutory requirements that inform this policy.

This policy applies to all members of the school community who access or use school digital systems, including staff, learners, governors, volunteers, parents/carers, visitors and community users. It applies to use of school systems both on and off site, and to the use of personal devices on the school site (where permitted).

Where online safety concerns or incidents occur outside school and are known to the school, Nant Celyn Primary will respond in line with this policy and related procedures, including the school's Safeguarding, Behaviour and Anti-Bullying policies. Where appropriate, parents/carers will be informed of incidents involving inappropriate online behaviour that take place out of school.

Policy development, monitoring and review

This policy has been developed by Nant Celyn Primary (e.g., Online Safety Group), drawing on the expertise and responsibilities across the school. Membership includes: (amend as appropriate)

- Headteacher / Senior leaders
- Designated Safeguarding Person (DSP)
- Online Safety Lead (OSL)
- Staff (including teaching, support and technical staff)
- Governors
- Parents/carers
- Community users (where relevant)

Consultation with the wider school community has taken place through a range of formal and informal opportunities to ensure the policy is understood, workable and proportionate.

Schedule for approval, monitoring and review

Approved by the Governing Body on: [08/10/2026]

Monitored by: Dean Davies (Deputy Headteacher)

Monitoring frequency: Annually

Reporting to the Governing Body: Annually

Policy review cycle: reviewed annually, or sooner in response to significant technological developments, emerging risks, or incidents.

Next planned review date: [*September 2027]*

Escalation following serious incidents: the school will inform relevant external agencies as appropriate, (e.g., *the Local Authority, Safeguarding Children's Board, and/or the police*).

Named contacts/agencies: *[D Davies – Deputy Headteacher, K Smith – Headteacher,]*

Monitoring the impact of the policy

The school will evaluate the effectiveness of this policy using evidence such as:

- Logs of reported online safety incidents
- Filtering and monitoring records
- Internal network activity monitoring data
- Surveys/questionnaires (as appropriate) of: Learners, Parents/carers, Staff

Policy and leadership

Responsibilities

Online safety is a shared responsibility. All members of the school community are expected to model safe, responsible behaviour, report concerns promptly and learn from incidents and good practice. The roles below clarify accountability.

Headteacher and senior leaders

Senior leaders set the culture and ensure that systems are effective. In line with Keeping Learners Safe the DSP holds day-to-day lead responsibility.

Senior leaders will:

- Ensure the school meets its safeguarding duty of care, including online safety.
- Know and apply procedures for serious allegations involving staff (Headteacher plus at least one senior leader).
- Ensure that the DSP/OSL, Education Technology Support Partner/technical staff and relevant colleagues are trained and able to fulfil their roles.
- ensure that children are taught about how to keep themselves and others safe online, recognising that effective education will be tailored to the specific needs and vulnerabilities of individual children.
- Put in place appropriate oversight and support for internal monitoring activity.

- Establish and receive regular online safety reports and act on emerging risks and themes.
- Work with governors, the DSP and IT provider on filtering and monitoring.

Governors

Governors approve the Online Safety Policy and challenge its effectiveness, in line with Keeping Learners Safe expectations.

The governing body will nominate an Online Safety Governor who will:

- Meet regularly with the DSP/OSL.
- Act as a critical friend challenging and supporting senior leaders to adequately assess cyber risks and implement robust policies and procedures.
- Receive anonymised incident and monitoring summaries.
- Check delivery of key commitments (e.g., education, reporting, staff training).
- Through regular review, assess the effectiveness of filtering and monitoring with SLT, DSP and Education Technology Support Partner, in line with the Education Digital Standards.
- Report to the relevant governor group/committee: *[Rebecca Driscoll]*
- Undertake basic cyber security awareness training and support school cyber security oversight.
- Participate in the Online Safety Group (where in place).

Governors also support parent/carer and community engagement in online safety.

Designated Safeguarding Person (DSP)

The DSP will:

- Lead safeguarding, including online safety, with clear responsibilities in their job description.
- Maintain up-to-date knowledge of online risks, filtering/monitoring and cyber security.
- Coordinate and record online safety concerns and incidents, escalating and referring in line with safeguarding procedures.
- Liaise with SLT, the Online Safety Governor, the Education Technology Support Partner and relevant external partners as required.
- Review anonymised incident patterns and filtering/monitoring information, confirming at least annual checks.
- Report regularly to SLT and drive continuous improvement across relevant policies and practice, using evidence (e.g. incident data, monitoring, self-review such as 360 safe Cymru).
- Ensure appropriate support for learners with additional learning needs (ALN).

Online Safety Lead (OSL)

The OSL will:

- Lead the Online Safety Group and support the DSP day to day.
- Lead development and review of online safety documentation.
- Coordinate awareness, staff confidence and reporting readiness through appropriate training
- Work with curriculum leads to map, embed and evaluate online safety education.
- Liaise with IT and pastoral/support teams.
- Maintain current knowledge of risks across content, contact, conduct and commerce.

Curriculum Leads

Curriculum leads will work with the DSP/OSL to deliver a planned online safety programme through appropriate channels, e.g. DCF, RSE, other curriculum areas, assemblies/pastoral provision and national initiatives e.g. Safer Internet Day.

Teaching and Support Staff

All staff are expected to uphold professional standards online and contribute to a strong safeguarding culture.

Staff will:

- Follow the Online Safety Policy, Safeguarding Policy, Technical Security Policy and sign/comply with the Staff AUA.
- Maintain professional boundaries (including online/remote learning).
- Supervise learner use of technology and follow procedures for online safety issues
- Embed online safety where appropriate; teach research skills, copyright and plagiarism awareness.
- Challenge harmful online behaviour and report concerns promptly.
- Use only school-approved digital services and AI tools; protect data, apply UK GDPR, and verify AI outputs for accuracy/bias before use.
- Complete induction and annual training, with updates as needed; contribute to improvement by sharing learning and concerns.

Education Technology Support Partner / technical staff

The Education Technology Support Partner supports leaders and the DSP to meet the Education Digital Standards. Where services are outsourced, the school remains accountable.

The Education Technology Support Partner / technical staff will:

- Maintain secure infrastructure and manage user access.
- Implement, maintain and update filtering and monitoring; provide reports; act on alerts and concerns.
- Support procurement, risk identification, reviews and checks with SLT/DSP.

- Monitor systems for misuse and report concerns promptly to Headteacher/ Deputy Headteacher
- Follow the school's Online Safety and Technical Security policies and keep technical knowledge current.

Learners

Learners will:

- Follow the Learner AUA and Online Safety Policy (including personal devices where permitted).
- Report concerns and know how to get help.
- Use technology responsibly, respecting others and their copyright and intellectual property.
- Use AI responsibly: protect original work, check accuracy and avoid plagiarism.
- Understand that out-of-school behaviour may be addressed where it affects the school community.

Parents and carers

Parents/carers are key partners in reinforcing safe online behaviour.

The school will:

- Publish the Online Safety Policy and share the learner AUA *(with local decisions on acknowledgement).*
- Provide guidance on the responsible use of online technologies and seek permissions for digital services/images where required.
- Share updates through meetings, newsletters, online channels and campaigns.

Parents/carers will be encouraged to reinforce key messages and support safe use of personal devices (where permitted in school).

Community users

Community users accessing school systems or platforms will sign a Community User AUA before access is provided. The school welcomes partnership working and shares good practice where appropriate.

Online Safety Group

The Online Safety Group provides strategic oversight of online safety, monitors implementation and impact of the Online Safety Policy, and ensures online safety is embedded across safeguarding, curriculum and technical practice. In some schools it may sit within a wider safeguarding or digital strategy group.

Membership *(amend as appropriate)*

- DSP, OSL, Senior Leader(s)
- Online Safety Governor
- IT/technical representative (internal or provider)
- Staff representatives (teaching/support)
- Learner representative(s)
- Parent/carer representative(s)
- Community/external partner (where relevant)

Core responsibilities

The group supports the DSP/OSL to:

- Draft, review and monitor the Online Safety Policy and related documents.
- Oversee filtering and monitoring, including requests for change.
- Map and review online safety education for breadth, progression and relevance.
- Review anonymised incident data and technical logs to identify trends and emerging risks.
- Gather feedback from learners, staff and parents/carers and turn this into improvement actions.
- Promote learner voice, peer support and awareness activity.
- Track and evidence improvement actions (e.g. 360 safe Cymru).

Governance and impact

- Operates to agreed Terms of Reference (membership, frequency, reporting lines), reviewed annually.
- Coordinates with Safeguarding, Behaviour, Curriculum, Digital Strategy and Learner Voice as needed.
- Reports key themes, actions and impact to SLT and governors, and shares appropriate summaries with the wider community.

Policy

Online Safety Policy

The Online Safety Policy is part of the school safeguarding framework and should be read alongside Safeguarding, Behaviour, Anti-Bullying and Data Protection policies.

What the policy does

- Defines responsibilities for online safety.
- Sets expectations for safe, professional and ethical use of technology (including AI).
- Sets out reporting, recording and response procedures for online safety incidents.
- Supports compliance with Keeping Learners Safe, Education Digital Standards and UK GDPR.
- Promotes learners' digital competence and critical understanding.

Implementation, monitoring and review

- Developed through the Online Safety Group and reviewed at least annually, and sooner if risks/technology change.
- Monitored by the DSL/OSL and governors using anonymised incident trends, filtering/monitoring reports and education review activity (e.g. 360 safe Cymru)
- Findings inform improvement planning and staff training priorities.

Communication and accessibility

- Shared at staff induction and reinforced through training.
- Communicated to learners and parents/carers through AUAs and awareness activity.
- Published on the school website.

Acceptable use

Acceptable use is defined through the Online Safety Policy and a suite of Acceptable Use Agreements (AUAs) *(see appendices).* AUAs matter most when they are understood, reinforced and followed—not simply signed.

Reinforcement

- staff and learner induction/handbooks
- on-screen reminders (e.g. splash screens), digital signage
- posters in areas where technology is used
- curriculum and awareness sessions
- communications with parents/carers
- school website

- peer support / learner-led activity

Schools should agree what is acceptable/unacceptable for their context (age, setting and systems) and record this in the tables below.

Acceptable/Unacceptable Actions

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
Users must not use online services (apps, games, sites) to create, share, download, upload, transfer or communicate material or comments that are:	Any illegal activity, for example: • Child sexual abuse imagery (CSAM)* • Child sexual abuse/exploitation and grooming • Terrorism-related content • Encouraging, promoting or assisting suicide/self-harm • Sexual image offences (including intimate image abuse/revenge porn and extreme pornography) • Incitement to, or threats of, violence • Hate crime • Public order offences (including harassment and stalking) • Drug-related offences • Weapons/firearms offences • Fraud and financial crime (including money laundering) *Note: follow UKSIC and UKCIS guidance when responding to self-generated intimate images (SGII).*					X
Users must not attempt or support cybercrime (Computer Misuse Act 1990), including:	• Misusing someone else's username/ID or password to access data, software or systems without authorisation • Gaining unauthorised access to school networks, data or files (including bypassing security controls) • Creating, introducing or spreading malware (viruses, ransomware, harmful scripts)					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
	• Phishing, credential theft, or attempting to capture passwords or personal data • Revealing, copying or publishing confidential information (e.g., personal/financial data, databases, access codes) • Disabling, impairing or disrupting network/services (e.g., denial of service) • Using penetration-testing tools without explicit permission *Note: schools should decide whether incidents are dealt with internally or reported to police. Serious or repeat offences should be reported. The National Crime Agency provides routes to divert young people away from cybercrime* and into positive pathways.					
Unacceptable (not illegal) under school policies, for example:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promoting discrimination, harassment or hateful content				X	
	Using school systems to run a private business or make unauthorised financial gain				X	
	Using tools/services to bypass filtering, monitoring or other safeguards (e.g., VPN/proxy, anonymisers, alternative DNS)				X	
	Infringing copyright or intellectual property (including via AI tools, stream ripping or unauthorised copying/sharing)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable & illegal
	Sharing content that is offensive, undermines the school's ethos, breaches integrity, or brings the school into disrepute				X	

Consider the following activities when used for non-educational purposes. Add or amend items to reflect current technology, age restrictions and your school's device policy.	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff oversight
Online gaming and in-game chat/voice (*e.g. Roblox, Fortnite, Minecraft*)	X							X
Online shopping and digital commerce (*including in-app purchases, marketplaces, subscriptions)*				X	X			
Cloud storage and file sharing (*e.g., Google Drive, OneDrive, Dropbox, WeTransfer; P2P/torrents*)		X				X		
Social media and user-generated platforms *(e.g. TikTok, Instagram, Snapchat, X, Reddit) and other age-restricted services*	X				X			

Consider the following activities when used for non-educational purposes. Add or amend items to reflect current technology, age restrictions and your school's device policy.	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff oversight
Messaging, chat and voice *(e.g., WhatsApp, iMessage, Snapchat, Discord, Teams personal accounts)*		X			X			
Streaming entertainment/media (video, music, podcasts) *e.g. Netflix, Disney+, Spotify*		X						X
Video platforms and livestreaming *(e.g. YouTube, Twitch, TikTok LIVE, Instagram Live)*		X						X
Personal mobile phones and smart devices on site *(phones, smartwatches, earbuds)*		X			X			
Mobile phones used for learning (teacher-directed and supervised)	X				X			
Mobile phones used during social time/breaks (where permitted) including device-free approaches		X			X			
Taking photos/video/audio on devices (including sharing, location data and consent)	X				X			

Consider the following activities when used for non-educational purposes. Add or amend items to reflect current technology, age restrictions and your school's device policy.	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff oversight
Other personal devices *(e.g., tablets, handheld consoles, VR headsets, wearables)*	X				X			
Personal email accounts on site or on the school network/Wi-Fi *(e.g., Gmail, Outlook.com)*		X			X			
School email used for personal communication (non-work/non-learning)			X		X			
Unapproved AI tools/services *(generative AI chatbots and image/video tools, AI companions, browser extensions)*			X		X			

Reporting and responding

Introduction

The school is committed to creating a culture where all members of the community feel confident, safe, and supported in reporting online safety concerns. In line with *Keeping Learners Safe*, the school recognises that online risks may occur in school or outside school and may affect children in any setting. Reporting routes must therefore be clear, accessible, inclusive, and consistently understood by all.

The school recognises national findings, including the Estyn Report – "we don't tell our teachers" - Experiences of peer-on-peer sexual harassment among secondary school pupils in Wales which

highlight that children may not always feel able to report. The school assumes that harmful online behaviours may be occurring, even where none have been disclosed, and responds by maintaining strong systems for reporting, analysing, and addressing concerns.

Reporting Concerns

The school will ensure that:

- Clear, accessible reporting routes are in place for all members of the school community, including pupils, staff, governors, parents/carers, and volunteers.
- Reporting processes are fully aligned with safeguarding procedures, including the child protection, whistleblowing, managing allegations and complaints policies.
- Multiple reporting options are available, such as speaking with the Designated Safeguarding Person (DSP), online or anonymous reporting tools (e.g., Whisper), email contact, or in-person disclosures.
- Reporting routes are well publicised through induction, assemblies, posters, the school website, and digital platforms.
- All users understand that any online safety concern must be reported, including those relating to harmful or illegal behaviour, sexual harassment, bullying, discrimination, grooming, or self-generated sexual imagery.

Responding to Concerns

The school will ensure that:

- Reports are acknowledged and responded to promptly, considering the safety and wellbeing of the person reporting.
- The DSP, Online Safety Lead, and senior leaders have the training and skills needed to recognise, assess, and manage online safety risks.
- Where a report indicates possible illegal activity or serious harm, it is escalated immediately through safeguarding procedures. Examples include (but are not limited to):
    - Child sexual abuse material (CSAM)
    - Non-consensual or self-generated images
    - Grooming, exploitation, or sexual harassment
    - Terrorism or extremism
    - Hate crime, fraud, extortion, stalking
    - Cyber offences under the Computer Misuse Act
    - Sale of illegal substances or goods
- Where concerns do not involve suspected illegal activity, devices may be checked using a safe, controlled, and documented process involving senior staff and a designated review device.
- AI-supported monitoring systems, where used, are subject to human oversight to ensure contextual understanding.
- Users who report concerns receive reassurance, appropriate support, and feedback on the outcome.

Recording and Monitoring

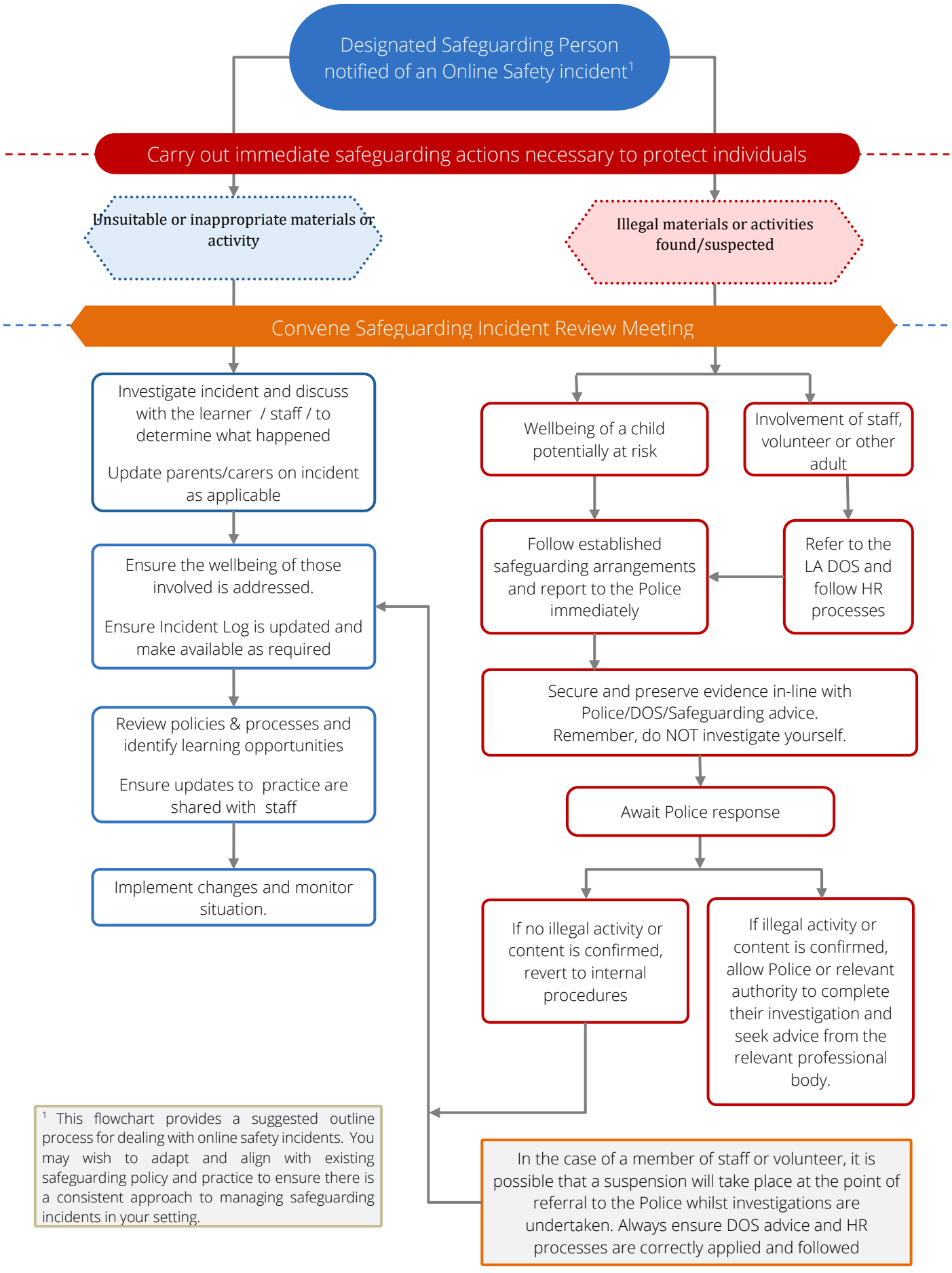
The school will:

- Maintain a secure and confidential record of all incidents, including actions, decisions, and follow-up.
- Ensure reports are audited and analysed regularly to identify emerging trends, patterns of concern, and the effectiveness of responses.
- Provide anonymised summaries of trends and learning to:
    - The Online Safety Group
    - Senior leaders
    - Governors (via safeguarding reports)
    - *Staff*
    - *Learners, where appropriate*
    - *Parents/carers through general communications*
    - *Local safeguarding partners, where relevant*

External Support and Escalation

The school will work with appropriate external agencies when required, including:

- Designated Officer for Safeguarding (DOS)
- Police / CEOP
- Local Safeguarding Children's Board
- Hwb – Keeping Safe Online – help and support



[1] This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.

Responding to Learner Actions

Incidents	Refer to class teacher/tutor	Refer to DSP / OSL	Refer to SLT	Refer to Police/Social Services	Refer to Education Technology Support Partner	Inform parents/carers	Issue a warning / intervention	Remove device / network /internet / access rights	Further sanction, in line with behaviour policy
Accessing illegal material (or attempting to), as defined in the earlier "Unsuitable/Inappropriate Activities" section.		X	X	X	X	X			
Unauthorised access to the school network, including using another person's account or sharing usernames/passwords.	X		X			X		X	X
Damaging, corrupting or deleting another user's data.	X		X		X	X	X	X	X
Sending offensive, harassing or bullying emails, texts or messages.		X	X			X	X	X	X
Unauthorised downloading/uploading, file sharing or distribution of files.	X		X		X	X	X	X	X
Bypassing filtering (e.g. proxy sites, VPNs or similar tools).		X	X		X	X	X	X	X
Failing to report accidental access to offensive or pornographic material	X	X	X			X	X		
Deliberately accessing offensive or pornographic material (or attempting to)		X	X	X	X	X		X	X
Sharing or receiving content that breaches copyright or data protection law.		X	X		X	X	X	X	
Unauthorised use of devices, including taking photos/videos or audio recordings.		X	X		X	X	X	X	X

Incidents	Refer to class teacher/tutor	Refer to DSP / OSL	Refer to SLT	Refer to Police/Social Services	Refer to Education Technology Support Partner	Inform parents/carers	Issue a warning / intervention	Remove device / network /internet / access rights	Further sanction, in line with behaviour policy
Unauthorised use of online services (apps, websites or platforms).		X	X		X	X	X		
Any online behaviour that could bring the school into disrepute or undermines the school's ethos.	X	X	X		X	X	X	X	X
Repeated breaches of these rules following previous warnings or sanctions.	X	X	X	X	X	X	X	X	X

Responding to Staff Actions

Incidents	Refer to line manager	Refer to SLT / Headteacher	Refer to LA	Refer to Police / DOS	Refer to Education Technology Support Partner	Issue a warning	Further Disciplinary action in line with Behaviour Policy
Accessing illegal material (or attempting to), as defined in the earlier "Unsuitable/Inappropriate Activities" section.		X	X	X	X	X	X
Breaching data protection or cyber-security requirements, including network security rules.		X	X	X	X	X	X
Accessing offensive or pornographic material (or attempting to).		X	X	X	X	X	X
Damaging systems or data, including corrupting/deleting others' data or deliberately damaging hardware/software.		X	X	X	X	X	X
Bypassing filtering controls (e.g. proxy sites, VPNs or similar methods).		X	X	X	X	X	X
Unauthorised downloading, uploading or file sharing.		X	X	X	X	X	X
Breaching copyright, licensing or intellectual property, including misuse of AI systems.		X	X	X	X	X	X
Unauthorised account/network access, including sharing passwords, using another person's account, or allowing others access.		X	X	X	X	X	X
Sending offensive, harassing or bullying emails, texts or messages.		X	X	X	X	X	X

Incidents	Refer to line manager	Refer to SLT / Headteacher	Refer to LA	Refer to Police / DOS	Refer to Education Technology Support Partner	Issue a warning	Further Disciplinary action in line with Behaviour Policy
Use of personal email/social media/messaging to communicate with learners or parents/carers.		X	X		X	X	X
Inappropriate personal use of school technology, including personal email and social media use during work time/using school systems.		X	X		X	X	X
Mishandling personal data, including storing, displaying or transferring it insecurely.		X	X	X	X	X	X
Any action that undermines professional conduct or a staff member's professional standing.		X	X	X	X	X	X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X	X			X	X
Failing to report incidents, whether accidental or deliberate.		X	X		X	X	X
Repeated breaches following previous warnings or sanctions.		X	X		X	X	X

Use of Artificial Intelligence (AI)

*A more detailed AI policy template (*Appendix C7*) is available, including an **AI risk assessment matrix** and an **AI-specific Staff Acceptable Use Agreement**.*

Generative AI (Gen AI) is developing rapidly and its use in education is increasing. In schools, AI is typically used in three areas: learner support, teacher support, and school operations. All use must be safe, ethical and responsible.

We recognise that Gen AI can introduce risks. These risks can be reduced through our existing safeguarding, data protection and technical security arrangements, and by updating procedures where needed. Safeguarding of learners and staff remains central to our approach.

Policy statements

The school will:

- Support appropriate use of AI to enhance learning and teaching, improve outcomes, streamline administration and reduce workload. Staff remain professionally responsible and accountable for any work supported by AI.
- Comply with relevant law and guidance, including Keeping Learners Safe and UK GDPR.
- Provide training and guidance for staff and governors on the benefits, risks and safe use of AI, and identify further development needs.
- Teach about AI through the curriculum where appropriate, helping learners understand how Gen AI works, its benefits and limitations, and its ethical and social impacts.

Safe use, data protection and security

The school will:

- Protect personal and sensitive data. Staff must not enter personally identifiable or sensitive information into AI tools. Where AI is used, staff should use anonymised data only.
- Require UK GDPR compliance. Staff must ensure any AI tool used meets data protection and security requirements before use.
- Approve tools and accounts. Only school-approved AI tools may be used for schoolwork, and staff should use school-provided AI accounts where available to support oversight and reduce risk.
- Safeguard sensitive information. Internal documents, strategic plans or other sensitive material must not be entered into third-party AI tools unless the tool and purpose have been explicitly approved.

Quality, fairness and integrity

The school will:

- Maintain human oversight. AI may support work but must not replace professional judgement—especially in decisions that affect people. AI outputs must be checked for accuracy before sharing or publishing.

- Promote transparency. Where AI has materially supported an output (e.g. documents, presentations, communications), staff should make this clear where appropriate.
- Address bias and discrimination. We recognise AI outputs may reflect bias. The school will use appropriate safeguards, review processes and procurement checks to prioritise fairness and safety.
- Protect copyright and intellectual property. The school will take steps to avoid copyright infringement and protect the intellectual property of staff and learners, including ensuring learners' work is not used to train AI systems without appropriate consent.

Reporting, monitoring and accountability

The school will:

- Require prompt reporting of AI-related concerns, including misuse, data incidents or inappropriate outputs, to Headteacher
- Maintain an inventory of AI tools in use, with purposes and risks recorded, and carry out regular review using the risk assessment matrices in Appendix C7.
- Engage parents/carers with clear information about how AI is used in school (e.g. an "AI in our school" guide).

Use in assessment and feedback

AI tools may be used to support teachers with assessment processes (e.g. identifying areas for improvement and drafting feedback), and to support learners in improving their work. Teachers remain responsible for outcomes and must ensure accuracy, fairness and appropriate use.

Misuse and disciplinary action

Improper use of AI - including breaches of this policy, data protection failures, misuse of sensitive information, or failure to follow agreed processes—may result in action under the school's Staff Disciplinary Policy.

Online Safety Education Programme

Online safety education is a core part of the school's safeguarding approach and sits alongside effective technical controls (including filtering and monitoring). In line with Keeping Learners Safe, online safety is a running and interrelated theme reflected across relevant policies and the Curriculum for Wales

The school delivers a planned, progressive and inclusive programme of online safety education for all learners, aligned to nationally recognised guidance and frameworks (including the Hwb Online safety policies and procedures and the Digital Competence Framework). Learning is age-

appropriate, builds on prior learning, is matched to need, and is taught through existing curriculum Areas of Learning and Experience (AoLE's) (including RSE, and Health and Well Being), with assessment and clear intended outcomes.

The programme develops learners' ability to:

- recognise and manage online risks, including harmful content, contact, conduct and commerce risks;
- understand consent, sexual harassment and sexual violence (including online), supported by safe opportunities for discussion;
- think critically about what they see online, including how to check reliability and accuracy and the role of AI-generated content;
- respect copyright and intellectual property, including when using online material and AI tools;
- understand and follow the learner acceptable use agreement, and act within moral and legal boundaries (including awareness of the Computer Misuse Act 1990).
- understand why online services use minimum-age requirements and how these may support safety, privacy and wellbeing
- make informed decisions about participation in social media, messaging, gaming and other online communities, including services they may not yet be permitted to use
- understand that legal or platform restrictions do not remove the need to learn about online relationships, harmful content, image sharing, scams, exploitation and digital wellbeing
- understand the school's mobile-phone requirements and the safeguarding, behaviour, learning and wellbeing reasons that underpin them.

Where internet use is planned, learners are guided to appropriate resources and supported if unsuitable content is encountered. Where open searching is permitted, staff supervise and remain vigilant. Filtering may be temporarily adjusted for legitimate curriculum research, with auditable approval and clear rationale.

Learner voice is actively used to strengthen the school's approach through feedback, learner representation (e.g. on an Online Safety Group), and opportunities such as digital leaders, peer mentoring, campaigns, and contribution to acceptable use and community-facing online safety activities. Learners are given appropriate opportunities to discuss changes affecting their digital lives and to express concerns about friendship, belonging, access, exclusion and wellbeing.

Staff

In line with Keeping Learners Safe all staff and volunteers receive safeguarding and child protection training, including online safety, at induction and through regular updates (at least annually).

Online safety training is integrated into the school's whole-school safeguarding approach, wider staff development and curriculum planning.

- All staff will receive online safety training and understand their responsibilities under this policy. Training will include (select/delete as appropriate):
- A planned programme of online safety, data protection and cybersecurity training for all staff, regularly updated and reinforced. Staff training needs will be reviewed periodically to ensure provision remains relevant and effective.
- Online safety training for all new staff as part of induction, ensuring understanding of the Online Safety Policy and Acceptable Use Agreements, including classroom management, professional conduct, online reputation and modelling positive online behaviour.
- Regular updates for the Designated Safeguarding Person (DSP) and Online Safety Lead (OSL) (or other nominated staff) through external training and review of relevant guidance (e.g. Hwb – Keeping Safe Online, UK Safer Internet Centre, SWGfL, Local Authority or other appropriate organisations).
- Support for staff knowledge-building and consistent practice through structured professional learning resources
- Regular review of this Online Safety Policy and updates through staff meetings, team briefings and/or INSET.
- Targeted advice, guidance and training from the DSP/OSL (or nominated staff) to individuals as required.
- The training ensures that staff:
    - understand the school's filtering and monitoring requirements, the responsibilities relevant to their role and how concerns or alerts must be reported
    - understand that filtering and monitoring support—but do not replace—effective supervision, professional curiosity and safeguarding judgement
    - understand and consistently apply the school's mobile-phone requirements, including expectations for their own professional use of personal devices.
    - know how authorised exceptions for learners are approved and managed
    - follow cyber security requirements

Governors

Governors should take part in online safety training and awareness activity. This is particularly important for governors serving on committees with responsibility for safeguarding, online safety, technology or health and safety.

Training and updates may be provided through (select/delete as appropriate):

- Guidance for Governors: Hwb: Cyber Crime, Cybersecurity, Online Safety; Keeping learners safe – module 5, UKSIC: Filtering and Monitoring
- Attendance at training offered by the Local Authority, or other relevant organisations (e.g. SWGfL).
- Participation in school training and information sessions (for example, staff briefings or parents' events). This may include attendance at assemblies or lessons where appropriate.
- Regular update meetings with the DSP and/or Online Safety Lead to review key themes, incidents and current priorities.

Enhanced training will be provided for (at least) the Online Safety Governor. This will include:

- Basic cyber security awareness training.
- Training to understand the school's filtering and monitoring provision, enabling effective participation in required checks and reviews.

External Stakeholders

Families, the wider community and external agencies play a vital role in supporting the online safety education and wellbeing of learners. The school recognises that parents and carers may have limited awareness of online risks so work to ensure parents are kept informed. Schools may also draw on external agencies to supplement the school's safeguarding approach. The school therefore works actively to build strong partnerships, share key messages, and ensure that families and the wider community are equipped to help keep children safe online.

The following principles underpin the school's engagement with external stakeholders:

Working with Parents and Carers

The school will support parents and carers to understand online risks, build confidence, and reinforce safe online behaviours at home. This includes:

- Regular communication and awareness-raising about online safety issues, curriculum content, and reporting routes.
- Providing information through newsletters, the school website, learning platforms, and digital communication tools.
- Offering opportunities such as parent/carer workshops, information events, or drop-ins focused on online safety.
- Involving learners in sharing online safety messages with parents/carers, including contributing to information events.

- Signposting parents and carers to trusted national resources (e.g. Hwb, UK Safer Internet Centre, Internet Matters, Childnet, SWGfL National Crime Agency
- Promoting and participating in key national events such as Safer Internet Day.
- Ensuring parents and carers understand acceptable use expectations and relevant school policies related to online safety.
- Clear information about the school's mobile-phone and other connected devices policies and arrangements, including the reasons for the policy, authorised exceptions and the consequences of breaches.
- Accurate, balanced and age-appropriate information about changes affecting social media and other online services
- Consultation and feedback to evaluate how well the school's approaches to mobile phones, online services and family engagement are working.
- guidance and support for parents on managing and supporting their children's online experiences and how to report and manage issues.
- guidance to help parents encourage their children to report online safeguarding concerns, regardless of any restrictions in place
- mechanisms that evaluate the efficacy of school's strategy on mobile phones, online services and family engagement

Wider Community and Agencies

The school recognises the value of working with external organisations to strengthen local online safety awareness and provision. This may include:

- Sharing online safety information, resources or updates with community groups, extended family members and the wider community.
- Providing or supporting family learning opportunities on digital technologies and safe online behaviours.
- Using the school website or social media channels to offer online safety content suitable for the broader community.
- Collaborating with early years settings, childminders, youth and sports groups, libraries, voluntary organisations or other local agencies.
- Drawing on the expertise of external agencies (e.g. UK Safer Internet Centre, CEOP, Local Safeguarding Partnerships, Prevent teams, police and health professionals).
- Participating in shared activities with other schools or settings, including transition projects and multi-school events.
- Supporting external groups to review and improve their own online safety practice.

Technology

Purpose

The school recognises that effective filtering, monitoring, technical security, cyber security and data protection are essential to safeguarding children and protecting the wider school community. These measures support safe and responsible use of technology while enabling effective teaching, learning and administration.

Detailed arrangements are set out in the Appendix C1 - Filtering and Monitoring Policy Template and Appendix C2 - Technical Security Policy Template.

Filtering and Online Safeguarding

The school has appropriate filtering and monitoring systems in place to help protect users from illegal, inappropriate and harmful online content and activity, in line with statutory guidance. (e.g., Hwb – Education Digital Standards, Keeping Learners Safe) and best practice guidance (e.g., UKSIC Appropriate Filtering and Monitoring)

The school ensures that:

- filtering and monitoring arrangements are safeguarding-led, proportionate and regularly reviewed
- filtering blocks illegal content and provides age-appropriate and role-appropriate access
- monitoring supports the rapid identification of safeguarding concerns and enables timely intervention
- all school-owned devices are subject to filtering and monitoring, including when used off-site
- staff and learners understand that filtering and monitoring are in place, why they are needed, and how concerns are escalated
- Where the use of personal devices is allowed, users understand that their use may be filtered and monitored by the school.

Oversight and Review

- Senior leaders, the Designated Safeguarding Person (DSP), Online Safety Lead (OSL) technical staff and governors have clear roles and responsibilities
- filtering and monitoring effectiveness is reviewed at least annually, and following significant changes or incidents. (e.g., using Testfiltering)
- log reports provide actionable information for safeguarding decisions.
- no system is relied upon in isolation; reporting routes and professional judgement remain central

Further detail is provided in the Appendix C1 - Filtering and Monitoring Policy Template

Technical Security

The school takes steps to ensure that its technical infrastructure is secure, reliable and well managed and meets its statutory requirements.

The school ensures that:

- access to systems and data is controlled through appropriate authentication and permissions
- devices, networks and systems are protected through secure configuration, patching and malware protection
- backups and recovery arrangements are in place to reduce the impact of system failure or attack
- incidents and weaknesses are reported, recorded and used to inform improvement
- responsibilities for technical security are clearly defined and supported by appropriate expertise
- systems are regularly reviewed and tested, meet statutory requirements and address emerging threats.

Further detail is provided in the Appendix C2 - Technical Security Policy Template.

Cyber Security

The school recognises cyber security as a leadership and governance responsibility and takes steps to reduce the risk and impact of cyber incidents. It recognises that cyber security is a safeguarding issue and not simply a technical issue.

The school ensures that:

- a cyber security approach is in place to prevent, detect, respond to and recover from cyber threats
- senior leaders and governors understand cyber risks and receive appropriate assurance
- staff and learners are educated/trained to recognise and report cyber security concerns
- business continuity and incident response arrangements are maintained and reviewed
- cyber security arrangements are kept under regular review and updated in line with emerging risks.

Further detail is provided in the Appendix C3 – Cyber Security Policy Template.

Data Protection

The school is committed to protecting personal data and complying with data protection legislation. (The Data (Use and Access) Act 2025 makes additional requirements on schools – particularly that online services accessed by learners meet higher protection standards)

The school ensures that:

- personal data is processed lawfully, fairly and transparently
- a Data Protection Officer (DPO) is appointed and appropriate governance arrangements are in place
- all staff receive regular training to ensure they are aware of their responsibilities and can respond appropriately to data protection incidents.
- systems are in place to respond effectively to Freedom of Information and Subject Access Requests
- Data Protection Impact Assessments have been conducted on existing and planned use of software and systems.
- privacy notices explain how data is used and how individual rights can be exercised
- data is stored, shared and disposed of securely
- data breaches are reported and managed in line with legal requirements
- data protection is embedded across safeguarding, teaching, learning and administration.
- where AI and Automated Decision-Making are in use, human oversight will be maintained for significant decisions, risk assessments will be conducted and the school will ensure automated systems are transparent and explainable.

Further detail is provided in the Appendix C4 – Data Protection Policy Template.

Review

Arrangements for filtering, monitoring, technical/cyber security and data protection are reviewed regularly and updated to reflect:

- changes in technology
- emerging safeguarding risks
- national guidance and statutory expectations

Technology Practice

Purpose

The school recognises that the safe and responsible day-to-day use of technology plays a vital role in safeguarding children, supporting learning, and protecting the school community. Clear expectations, consistent practice and informed users help reduce risk while enabling positive and purposeful use of digital technologies.

This approach supports the safeguarding duties set out in Keeping Learners Safe emphasising safeguarding and whole-school responsibility, including the requirement to address online safety through policy, practice, education and staff training.

Detailed arrangements are set out in the relevant policy appendices, including the Technical Security, Cyber Security, Data Security, Filtering and Monitoring, Device Management and Public Online Communications templates.

Device Management

The school manages the use of digital devices in a way that supports safeguarding, learning and responsible behaviour. This reflects Keeping Learners Safe requirements for a clear mobile / smart technology policy and explicitly links device use to behaviour, safeguarding and education

The school ensures that:

- expectations for the use of school-owned and personal devices are clearly defined and communicated
- device use is consistent with safeguarding, behaviour, data protection and acceptable use policies
- appropriate technical and procedural controls are in place to support safe use
- staff, learners and visitors have been trained/educated/informed and understand their responsibilities when using devices on school premises or systems
- education on the safe and responsible use of devices forms part of the school's online safety education
- there are clear policies about learners access to mobile phones or other personal smart devices during the school day
- any exceptions to the mobile phone and other digital devices policy are limited, clearly defined, authorised and managed appropriately, for example where required for medical, safeguarding, accessibility or ALN-related reasons
- staff model the school's requirements and use personal devices only where authorised and professionally appropriate
- procedures cover possession, storage, confiscation, searching and return of devices, in accordance with school policy and relevant guidance.

Decisions about device use are informed by risk assessment and reviewed regularly.

Digital Content

The school recognises that multi-modal digital content (inc. AI) can enrich learning and communication when used responsibly. Its approach supports safeguarding requirements in particular, sexual imagery, consent, coercion, privacy and the sharing or manipulation of content.

The school ensures that:

- clear expectations are in place for the creation, use, storage and sharing of digital content
- consent, privacy and safeguarding considerations are applied consistently
- staff and learners are trained/educated to understand their responsibilities when creating or sharing digital content
- personal data and images are handled securely and lawfully
- school-approved platforms and accounts are used where content includes personal or sensitive information
- staff and learners understand that content may be copied, altered, republished or distributed beyond its intended audience, including through AI technologies
- AI-generated or AI-assisted content is reviewed for accuracy, legality, appropriateness, bias, transparency, copyright and safeguarding risk before use or publication
- School staff are aware of and understand: advice and guidance to support education settings to understand and respond to emerging safeguarding risks associated with AI.
- policy and practice are reviewed in the light of emerging technologies and risks.

Public Online Communications

The school uses public online communications to inform, celebrate success and engage with the wider community, while managing associated risks. It supports Keeping Learners Safe expectations around professional boundaries and staff conduct online, addresses reputational and safeguarding risk from public platforms while reinforcing parental engagement and transparency.

The school ensures that:

- public online communications are appropriate, accurate and well-managed
- public communications from or regarding the school are monitored and addressed where appropriate
- published content complies with safeguarding, data protection and statutory requirements
- to reduce the risk of illegal manipulation of publicly available images of staff and learners, the school has procedures in place to control how those images are shared online. (Hwb guidance on web scraping)
- publishing public communications is restricted to authorised and trained staff
- AI-assisted public communications are checked by an appropriately responsible person before publication and remain subject to human accountability
- online safety information is shared with parents, carers and the wider community
- clear processes exist for managing school online accounts
- staff understand expectations around professional conduct and online behaviour
- the school communicates confirmed changes to policy in line with best practice and Government guidance.

Review

Technology practice is reviewed regularly to reflect:

- changes in technology and online behaviour
- emerging safeguarding risks
- feedback from staff, learners and parents
- national guidance and statutory expectations

Outcomes

The impact of the Online Safety Policy and practice is evaluated regularly using evidence such as online safety incident logs, behaviour and bullying records, and surveys of staff, learners and parents/carers. Evaluating student outcomes as part of their online safety should be defined and evaluated as part of the school's assessment processes. Findings are reported to relevant groups and used to strengthen practice.

This process ensures that:

- evidence from audits and reviews is discussed through balanced professional debate, alongside the impact of preventative work (education, awareness and training)
- clear reporting routes are in place so patterns, themes and outcomes are shared regularly with senior leaders and governors
- parents/carers are informed of key patterns and learning through the school's online safety communication and awareness activity
- online safety and related policies and procedures are updated in response to evidence and emerging risks
- learning and evidence of impact are shared, where appropriate, with other schools, agencies and local authorities to support a consistent local approach to online safety.

List of appendices

Copies of the more detailed template policies and agreements, contained in the appendix, can be found in the links and resources section of the relevant aspects in the 360safe self-review tool and online in Keeping Safe Online on Hwb

The appendices are as follows:

A1 - Learner Acceptable Use Agreement Template – for older learners
A2 - Learner Acceptable Use Agreement Template – for Primary learners
A3 - Learner Acceptable Use Agreement Template – for younger learners
A4 - Parent/Carer Acceptable Use Agreement Template

A5 - Staff (and Volunteer) Acceptable Use Policy Agreement Template
A6 - Community Users Acceptable Use Agreement Template
A7 – Online Safety Policy Statement Template
A8 - Harmful Sexual Behaviour Policy Template
A9 - Computer Misuse and Cyber Choices Policy Template
A10 - Responding to incidents of misuse – flow chart
A11 - Record of reviewing devices/internet sites (responding to incidents of misuse)
A12 - Reporting Log
B1 - Training Needs Audit Log
C1 – Filtering and Monitoring Policy Template
C2 - Technical Security Policy Template (including Access, Device and Incident Management)
C3 - Cyber Security Policy Template
C4 - Data Protection Policy Template
C5 – Public Online Communications Policy Template
C6 – Use of Artificial Intelligence (AI) in Schools Policy Template
Legislation
Links to other organisations and resources

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice, and guidance have contributed to the development of this school Online Safety Policy template and of the 360 safe online safety self-review tool:

Copyright of these policy templates is held by SWGfL. Schools and other educational institutions are permitted free use of the policy templates for the purposes of policy review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (onlinesafety@swgfl.org.uk) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in August 2026. However, SWGfL cannot guarantee it's accuracy, nor can it accept liability in respect of the use of the material.

© SWGfL 2026

Appendix A1 - Learner Acceptable Use Agreement Template – for older learners

Sections that include advice or guidance are written in BLUE. Schools should review and amend the contents of this agreement to ensure that it is consistent with their online safety policy and other relevant school policies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users.

Learner Acceptable Use Agreement Form

I agree to use the school's digital system, devices and online services responsibly to protect my safety, the security of the school systems, and others.

Personal Safety

- The school will monitor my use of its digital systems, devices, online services and communications.
- I will keep my usernames and passwords secure and private. If compromised, I will report or change them immediately.
- I will only share personal information, like my name or address, when absolutely necessary and with permission.
- I will be cautious when meeting online contacts in person, only doing so with a trusted adult in a public place.
- I will take responsibility for my actions online, using tools like blocking, reporting or ending chats if needed.
- I will share images of myself or others only when it is safe and will ensure the images are appropriate and respectful.
- I will only take or share images of myself, or others, when fully dressed. I understand that sharing nude or semi-nude content can cause distress, may be illegal and could lead to prosecution / criminal records.
- I understand that images and videos can be copied, altered (including using AI) and shared beyond my control.

- I will report harmful or unpleasant material, messages, or anything that worries or upsets me to a trusted adult.

Respecting Others' Work and Information

- I will seek permission before using or adapting someone else's work.
- I will verify information I find online, as it may not always be accurate or truthful.
- I will only use Artificial Intelligence (AI) tools approved by the school and ensure my use is ethical, legal, and transparent.
- I will check AI-generated content carefully, recognising that it may be inaccurate, misleading or biased, before using or sharing it.
- When I use generative AI to assist in creating digital content, I will ensure it is labelled as such.
- I will avoid downloading or using copyrighted or protected materials without proper permissions.

Responsible Online Behaviour

- I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not bully, harass, threaten, upset or make fun of others.
- I will only use platforms or software approved by the school and will not attempt to bypass the filtering/security systems in place. If I become aware of any such attempts, I will report this to a trusted adult.
- I understand that cyber security risks can include phishing, scams, AI-generated content and fake messages. I will think carefully before opening links, sharing information or responding to unexpected requests.
- I will immediately report any damage, faults or failings involving equipment or software, however this may have happened.
- I will follow the school's requirements for using mobile phones and other personal devices and respect the minimum age requirements for social media, apps and online services.
- I understand that age restrictions are designed to help protect children and young people. If I use online services, I will do so safely, responsibly and in accordance with school requirements.
- I will balance my online and offline activities to promote a healthy lifestyle.
- I will protect my online reputation and that of the school, its staff, and other learners.
- I will ensure my behaviour reflects positively on the school, both in and out of school settings.

- I understand that some online behaviours might be regarded, by some, as fun but can have serious consequences – this might include taking (or sharing) images/videos of staff, fights, learners in embarrassing situations or the setting up of fake accounts.
- I know I can talk to a trusted adult if I am worried about anything I see or experience online, even if I think I may have broken one of these rules.

Consequences of Misuse

- I understand that failing to follow this agreement may lead to consequences, including loss of access to the school's systems, detentions, suspensions, contacting parents/carers, or involvement of the police in serious cases.

By following these guidelines, I will contribute to a safe, respectful, and productive online environment.

I have read and understand the above and agree to follow these guidelines when:

- I use the school's systems and devices (both in and out of school)
- I use my own devices in the school (when allowed)
- I use digital technologies out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website etc.

(Schools will need to decide if they require learners to sign, or whether they wish to simply make them aware of acceptable use through education programmes/awareness raising).

Name of Learner: ..... Group/Class: .....

Signed: ..... Date: .....

Parent/Carer Countersignature (optional)

It is for schools to decide whether or not they require parents/carers to sign the parent/carer acceptable use agreement (see template later in this document). This includes a number of other permission forms (including digital and video images/biometric permission/cloud computing permission).

Some schools may, instead, wish to add a countersignature box for parents/carers to this learner acceptable use agreement.

Appendix A2 - Acceptable Use Agreement Template – for Primary Learners

Sections that include advice or guidance are written in BLUE. Schools should review and amend the contents of this agreement to ensure that it is consistent with their online safety policy and other relevant school policies.

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

I agree to use the school's digital systems, devices and online services safely and responsibly to protect me, other learners and the school.

Keeping Safe Online

- The school will check how I use devices and online services to keep everyone safe.
- I will keep my usernames and passwords private and tell a trusted adult if someone else knows them.
- I will be careful when talking to people online and will only talk to people I know and trust.
- I will not share personal information like my name, address, or photos without asking a trusted adult.
- I will only take or share images of myself, or others, when fully dressed.
- If I see or hear something online that worries or upsets me, I will tell a trusted adult straight away.
- I will only meet people I have spoken to online if a trusted adult is with me.

Using Devices and Online Services Sensibly

- I will only use devices, apps, games and websites that my teacher or parent/carer says are suitable for my age.
- I know that I am not allowed to use some online services and I know what these are.
- I will always ask permission and check with a trusted adult before using someone else's work or pictures.

- I will make sure the information I find online is true by checking carefully.
- I will only use apps or tools, like AI, that my teacher has said are OK, and I will ask for help if I'm unsure.
- I will not copy or use music, videos, or games unless I have permission.
- I will tell a trusted adult about any damage to devices or if anything else goes wrong.
- I will check with trusted adults before clicking on any unexpected messages or links (even if these look as though they are from people that I already know).

Being Respectful and Responsible

- I will treat others kindly online, just as I do in real life.
- I will make good choices about what I share online to protect myself and others.
- I understand that not every app or website is suitable for children my age.
- If I want to join a new app, game or online community, I will speak to a trusted adult first.
- I will spend a healthy amount of time using devices and make time for other activities too.
- I will always think about how my behaviour online could affect me, my friends, and my school.
- If I make a mistake online, I know I can ask a trusted adult for help.

What Happens If I Break These Rules?

- If I don't follow these rules, my teacher may stop me from using computers or devices, speak to my parents or carers, or take other actions to help me make better choices in the future.

By following these rules, I can enjoy using technology safely and responsibly.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner: ..... Group/Class: .....

Signed: ..... Date: .....

Schools will need to decide if they require learners to sign, or whether they wish to simply make them aware through education programmes/awareness raising.

Parent/Carer Countersignature (optional)

It is for schools to decide whether or not they require parents/carers to sign the parent/carer acceptable use agreement (see template later in this document in the Parent/Carer AUA). This includes a number of other permission forms (including digital and video images/biometric permission/cloud computing permission).

Some schools may, instead, wish to add a countersignature box for parents/carers to this learner acceptable use agreement.

Appendix A3 - Acceptable Use Agreement Template – for younger learners

Our Technology Rules

I will follow these rules to use computers, tablets and the internet safely at school. These rules help us all stay safe and have fun using computers and tablets at school!

Staying Safe

- My teacher will watch what I do on computers, tablets and the internet to keep me safe.
- I will keep my passwords secret and tell my teacher if I need help.
- I understand that people online are not always who they say they are. I will only talk to people online if my teacher or a trusted adult says it's OK.
- I will not share my name, address, or pictures without asking my teacher or a trusted adult first.
- If I see something that makes me feel worried or upset, I will tell my teacher or a trusted adult straight away.
- I will only use apps and games that a trusted adult says are right for me.
- If I want to try a new game or app, I will ask a trusted adult first.

Using Technology Kindly

- I will be kind when using technology, just like I am in real life.
- I will take care of the computers and tablets I use.
- I will only look at things my teacher says are OK.

Making Good Choices

- I will ask my teacher before I use someone else's pictures or work.
- I will take breaks from screens and do other fun things too.
- I know that I can say no / please stop to anyone online who makes me feel sad, uncomfortable, embarrassed or upset.
- If something goes wrong or if I am not sure what to do, I will tell my teacher or a trusted adult because they are there to help me.

What Happens If I Forget the Rules

- If I forget the rules, my teacher will help me learn to make better choices next time.

Signed (child): .....

(The school will need to decide whether or not they wish the children to sign the agreement – and at which age - for younger children the signature of a parent/carer should be sufficient)

Signed (parent): .....

Appendix A4 - Parent/Carer Acceptable Use Agreement Template

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open new opportunities for everyone. They can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that learners have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users. A copy of the learner acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.
Parents and carers are requested to sign the permission form below to show their support of the school in this important aspect of the school's work. (Schools will need to decide whether they wish parents and carers to sign the acceptable use agreement on behalf of their child)

Permission Form

Parent/Carers Name: .....

Learner Name: .....

As the parent/carer of the above learner, I give permission for my child to have access to the digital technologies at school.

I understand that the school has discussed the acceptable use agreement with my child and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems.

I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using devices.

I understand that my child's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of digital technologies at home and will inform the school if I have concerns over my child's online safety.

As the schools is collecting personal data by issuing this form, it should inform parents/carers as to:

This form (electronic or printed)
Who will have access to this form.
Where this form will be stored.
How long this form will be stored for.
How this form will be destroyed.

Signed: .....

Date: .....

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Learners and members of staff may record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared names will not be published and where possible the use of images "face-on" will be avoided.

The school will comply with the Data Protection Act and request parent's/carer's permission before taking images of members of the school.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal

use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their child and for the parents/carers to agree.

As the schools is collecting personal data by issuing this form, it should inform parents/carers as to:

This form (electronic or printed)	The images
Who will have access to this form.	Where the images may be published. e.g. Social Media, website, local press, etc. (see relevant section of form below)
Where this form will be stored.	Who will have access to the images.
How long this form will be stored for.	Where the images will be stored and for how long
How this form will be destroyed.	How the images will be destroyed.
	How a request for deletion of the images can be made.

Digital/Video Images Permission Form

Parent/Carer's Name:..... Learner's Name:.....

As the parent/carer of the above learner, I agree to the school taking digital/video images of my child/children.	Yes/No
I agree to these images being used:	
• to support learning activities.	Yes/No
• in publicity that reasonably celebrates success and promotes the work of the school.	Yes/No

Insert statements here that explicitly detail where images are published by the schools	Yes/No
I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes/No

Signed: .....

Date: .....

Use of Cloud Systems Permission Form

Schools that use cloud hosting services may be required to seek parental permission to set up an account for learners.

Schools will need to review and amend the section below, depending on which cloud hosted services are used.

The school uses **insert cloud service provider name** for learners and staff. This permission form describes the tools and learner responsibilities for using these services.

The following services are available to each learner as part of the school's online presence in **insert cloud service provider name**

Using **insert cloud service provider name** will enable your child to collaboratively create, edit and share files and websites for school related projects and communicate via email with other learners and members of staff. These services are entirely online and available 24/7 from any internet-connected computer.

The school believes that use of the tools significantly adds to your child's educational experience.

As the school is collecting personal data and sharing this with a third party, it should inform parents/carers about:

This form (electronic or printed)	The data shared with the service provider
Who will have access to this form.	What data will be shared and with whom
Where this form / data will be stored.	Who will have access to the data.
How long this form will be stored for.	Where the data will be stored and for how long
How this form will be destroyed.	How a request for deletion of the data can be made.

Do you consent to your child to having access to cloud services? Yes/No

Learner Name: ..... Parent/Carers Name: .....

Signed: ..... Date: .....

Use of Biometric Systems in England and Wales

If the school uses biometric systems (e.g. fingerprint/palm recognition technologies) to identify children for access, attendance recording, charging, library lending etc it must (under the "Protection of Freedoms" and Data Protection legislation) seek permission from a parent or carer.

The school uses biometric systems for the recognition of individual children in the following ways (the school should describe here how it uses the biometric system).

Biometric technologies have certain advantages over other automatic identification systems as learners do not need to remember to bring anything with them (to the canteen or school library) so nothing can be lost, such as a swipe card.

The school has carried out a data privacy impact assessment and is confident that the use of such technologies is effective and justified in a school context.

No complete images of fingerprints/palms are stored and the original image cannot be reconstructed from the data. Meaning that it is not possible, for example, to recreate a learner's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

As the school is collecting special category personal data and **delete as appropriate** sharing this with a third party, it should inform parents/carers about:

This form (electronic or printed)	The data shared with the service provider
Who will have access to this form.	What data will be shared and with whom
Where this form / data will be stored.	Who will have access to the data.
How long this form will be stored for.	Where the data will be stored and for how long
How this form / the data will be destroyed.	How consent to process the biometric data can be withdrawn.

Parent/Carers Name: .....

Learner Name: .....

As the parent/carer of the above learner, I agree to the school using biometric recognition systems, as described above. Yes/No

I understand that the images cannot be used to create a whole fingerprint/palm print of my child and that these images will not be shared with anyone outside the school. Yes/No

Signed: .....

Further guidance

- Each parent of the child should be notified by the school that they are planning to process their child's biometrics and notified that they are able to object.
- In order for a school to process children's biometrics at least one parent or carer must consent and no parent or carer has withdrawn consent. This needs to be in writing.
- The child can object or refuse to participate in the processing of their biometric data regardless of parent or carer's consent.
- Schools must provide reasonable alternative means of accessing services for those learners who will not be using an automated biometric recognition system.
- Permission only needs to be collected once during the period that the learner attends the school, but new permission is required if there are changes to the biometric systems in use.

Learner Acceptable Use Agreement

On the following pages we have copied, for the information of parents and carers, the learner acceptable use agreement.

It is suggested that when the learner AUA is written that a copy should be attached to the parents/carers acceptable use agreement to provide information for parents and carers about the rules and behaviours that learners have committed to by signing the form.

Appendix A5 - Staff (and Volunteer) Acceptable Use Agreement Template

Sections that include advice or guidance are written in BLUE. Schools should review and amend the contents of this agreement to ensure that it is consistent with their Online Safety Policy and other relevant school policies.

School Policy

Digital technologies have become integral to the lives of everyone, including children and young people, both within schools and in their lives outside school. The internet and digital technologies are powerful tools, which can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. The school has the right to protect itself and its systems and all users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while online and using digital technologies for educational, personal and recreational use
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities and will, in return, expect staff and volunteers to agree to be responsible, informed and professionally competent users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to minimise the risk to the safety, privacy or security of the school community and its systems. I acknowledge the potential of digital technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos and values.

For my professional and personal safety:

- I understand that filtering and monitoring are safeguarding measures designed to protect learners, staff and school systems. Where my role requires it, I will act promptly on concerns or alerts in accordance with the school's safeguarding procedures.
- I understand that the rules set out in this agreement also apply to use of these devices and technologies out of school, and to the transfer of personal / sensitive data (digital or paper based) out of the school

- I understand that the school devices and digital technology systems are primarily intended for educational use and that I will only use them for personal or recreational use within relevant school policies.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will store my passwords securely and in line with the school's relevant security policy.
- I will immediately report any safeguarding, cyber security, filtering, monitoring or data protection concern using the school's agreed reporting procedures.
- I will complete the online safety, safeguarding and cyber security training required by the school and keep my knowledge up to date.

I will be professional in my communications and actions when using digital technologies and systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images, and taking account of parental permissions. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in the school in accordance with school policies.
- I will only communicate with learners, parents/carers and colleagues using school-approved systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

Protecting Learners, School Systems and Information

- I will abide by all relevant guidance and legislation (e.g. Keeping Learners Safe and UK GDPR).
- I will ensure that I am aware of cyber-security risks and that I will not respond to any communications that might put my / school data or systems at risk from attack.
- I will not connect or used unauthorised USB drives or other external storage devices, as they may contain malware of viruses that could compromise the security of school systems and data.
- When using AI systems in my professional role I will use these responsibly and:
  - will only use AI technologies approved by the school

- will be aware of the risks of bias and discrimination, critically evaluating the outputs of AI systems for such risks
- to protect personal and sensitive data, I will ensure that I have explicit authorisation when uploading sensitive school-related information into AI systems
- will take care not to infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance
- critically evaluate AI-generated outputs to ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing
- will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identity and well-being
- I recognise that AI supports, but does not replace, my professional judgement. I remain responsible for the accuracy, appropriateness and safeguarding implications of any AI-assisted work.

- I will follow the school's expectations and policies for the professional use of mobile phones and other connected devices, ensuring only permitted use
- When communicating in a professional capacity, I will only use technology and systems sanctioned by the school.
- I will not use personal accounts on school systems.
- I will exercise informed safe and secure practice when accessing links to content from outside of my organisation to reduce the risk of cyber security threats.
- I will help protect school systems by following the school's cyber security procedures.
- I will not access illegal, inappropriate or harmful content on school systems.
- I will respect filtering, monitoring and other security measures and report any concerns about their effectiveness.
- I understand that some websites or services may be restricted for safeguarding reasons and will use the school's agreed process where access is required for legitimate educational purposes.
- I will not install or attempt to install unauthorised programmes of any type on a school device, nor will I try to alter device settings, unless this is allowed in school policies
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school Data Security Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that the data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that

I am required by law or by school policy to disclose such information to an appropriate authority.

- I will only use school-approved cloud services and digital platforms for storing or sharing school information.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using digital technologies in my professional capacity or for school sanctioned personal use:

- I will ensure that I have appropriate permissions to use the original work of others in my own work and will reflect this with appropriate acknowledgements, particularly where AI has been used to generate content
- Where content is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that my professional responsibilities extend to my conduct in public online spaces where this could affect learners, colleagues or the reputation of the school.
- I will ensure my use of technologies and platforms is in line with the school's agreed codes of conduct.
- I will model safe, responsible and balanced use of digital technology in my professional practice.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include (schools should amend this section to provide relevant sanctions as per their behaviour policies) a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities, the involvement of the Police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of the school) and my own devices (in the school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: .....

Signed: .....

Date: .....

Appendix A6 - Acceptable Use Agreement for Community Users Template

This acceptable use agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, whatever the cause.
- I will ensure that I have permission to use the original work of others in my own work

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices

I have read and understand the above and agree to use the school systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

As the school is collecting personal data by issuing this form, it should inform community users about:

Who will have access to this form.	How this form will be destroyed.
Where this form will be stored.	How long this form will be stored for.

Name: ..... Signed: ..... Date: .....

Appendix A7 - Online Safety Policy Statement

At [School name], we want every user to be safe, confident and supported when using technology - whether learning in school, at home, or in the wider community. Online safety is part of safeguarding and wellbeing. It is not "just an IT issue": it is about people, relationships, behaviour, learning, and protection.

Our online safety strategy is built around four outcomes-focused areas that strengthen day-to-day practice:

- Leadership and policy that make expectations clear
- Education that builds skills, resilience and positive behaviour
- Technology that protects users and supports safe learning
- Impact review that proves what's working and what we will improve

Leadership and policy: clarity, consistency and accountability

- When leadership is strong, online safety becomes part of "how we do things here"—not a one-off initiative.

Clear responsibilities

- We make sure roles are defined and understood across senior leaders, the Designated Safety Person, an Online Safety Lead, governors and technical staff/providers. This ensures safeguarding decisions and technical safeguards work together.
- What this improves: decisions are quicker, concerns are escalated correctly, and actions don't get "lost" between teams.
- Benefit for users: children and adults get safer, more consistent support.

A joined-up Online Safety Group

- We involve the right voices—leaders, staff, governors, and (where appropriate) learners and families—to keep online safety responsive to real experiences and emerging risks.
- What this improves: shared ownership and a whole-school approach.
- Benefit for users: safer practice is reinforced across school and home.

A policy that is understood and used

- Our online safety policy is aligned with safeguarding expectations and linked to related policies so that staff and families can see one clear, consistent approach.
- What this improves: fewer grey areas and more confident decision-making.
- Benefit for users: clear boundaries and predictable responses.

Acceptable use expectations that protect everyone

- We set out simple, age-appropriate expectations for learners and clear professional expectations for staff, so everyone understands what safe and respectful use looks like.

- What this improves: behaviour, consistency, and fairness.
- Benefit for users: safer online spaces and fewer harmful incidents.

Reporting and responding that leads to action

- We promote a culture where people feel able to speak up, and we respond consistently, recording concerns, acting promptly, and learning from patterns and new risks.
- What this improves: early identification and effective safeguarding intervention.
- Benefit for users: children get help sooner; everyone feels listened to and protected.

Education: confident learners and informed adults

- We teach online safety to build knowledge, skills, attitudes and resilience—so learners can enjoy the benefits of technology while managing risks.

Planned learning for learners

- Online safety education is progressive, inclusive and revisited regularly. We use learner voice to shape what we teach and to keep it relevant.
- What this improves: safer choices, healthier online behaviour, and confident help-seeking.
- Benefit for users: learners become better prepared for real-life online challenges.

Staff training that supports safeguarding practice

- All staff receive induction and ongoing updates so they can spot concerns, respond appropriately, and model safe practice. Key roles receive enhanced training to lead and make informed decisions.
- What this improves: confidence and consistency across the workforce.
- Benefit for users: concerns are handled calmly, correctly and promptly.

Governors trained to provide challenge and support

- Governors understand their duties and can ask the right questions about policy, training, curriculum, filtering/monitoring, and cyber security.
- What this improves: accountability and sustained improvement.
- Benefit for users: online safety stays a priority over time, not just after incidents.

Strong partnerships with families and agencies

- We communicate practical guidance to families and work with relevant partners. We also share effective practice beyond our school where it supports safer communities.
- What this improves: joined-up messages and earlier support.
- Benefit for users: children experience consistent expectations across school and home.

Technology: protection that enables learning

- We use proportionate technical controls to reduce exposure to harm while supporting teaching and learning.

Effective filtering

- Filtering reduces the risk of access to harmful and illegal content and is reviewed to ensure it stays fit for purpose.
- Benefit for users: safer browsing and research.

Safeguarding-led monitoring

- Monitoring helps identify concerns early and supports timely intervention, handled with appropriate governance and data protection.
- Benefit for users: timely intervention when risk is emerging.

Secure systems and cyber resilience

- We protect networks, devices and accounts, and we prepare for threats like phishing and ransomware—so learning is not disrupted and users are protected.
- Benefit for users: safer services, fewer incidents, faster recovery.

Data protection that builds trust

- We handle personal and sensitive information carefully and lawfully, with clear processes and accountability.
- Benefit for users: privacy is respected and risks from misuse are reduced.

Safe day-to-day practice

- We manage devices consistently (including expectations around personal devices where relevant), apply safeguarding and consent to digital content, and communicate responsibly through our public channels.
- Benefit for users: fewer avoidable mistakes and a safer, more responsible digital culture.

Impact: proving what works and improving what doesn't

- We regularly review how well our policies and practice are working, what the evidence tells us, and what we will improve next. This keeps our approach current, targeted and effective.

How to raise a concern or get help

If something online worries you, we want to know.

- Learners: talk to a trusted adult, your tutor/class teacher or teaching assistant, or the safeguarding team.
- Parents/carers: contact [DSP name / safeguarding email/phone].
- Staff: follow safeguarding procedures and record concerns promptly.

Our commitment

We will keep strengthening leadership, education, technology and impact review so that technology at [School name] is used safely, respectfully and positively—and so our community can be confident that online safeguarding is robust, consistent, and always improving.

Appendix A8 - Harmful Sexual Behaviour Policy Template (New)

Purpose

The school recognises that harmful sexual behaviour may be happening but not reported and that it increasingly occurs online involving image sharing, coercion, exploitation and anonymous abuse.

The purpose of this policy is to set out the school's approach to preventing, identifying and responding to Harmful Sexual Behaviour (HSB), sexual harassment and sexual violence between children.

This policy forms part of the school's safeguarding framework and should be read alongside other relevant policies.

The school adopts a zero-tolerance approach to harmful sexual behaviour in line with national safeguarding guidance (see list below)

Scope

This policy applies to:

- All learners, staff, volunteers and governors
- Behaviour occurring within and outside school where it impacts the school community

Legislative and National Context

This policy reflects national guidance including:

- Keeping Learners Safe
- Estyn - We don't tell our teachers – Experiences of peer-on-peer sexual harassment among secondary school pupils in Wales
- Violence Against Women, Domestic Abuse and Sexual Violence (Wales) Act 2015
- Hwb - Sharing Nudes and Semi-Nudes Guidance

Roles and Responsibilities

- Governors provide strategic oversight, ensure annual review of this policy and monitor safeguarding trends.
- Senior Leaders promote a culture of respect and equality and ensure consistent implementation and staff training.
- The Designated Safeguarding Person (DSP) leads responses to incidents, ensures safeguarding procedures are followed, completes risk assessments and liaises with external agencies.
- All staff must challenge inappropriate behaviour, report concerns immediately to the DSP and respond to disclosures in a calm and supportive manner.

Policy Statement

The school will ensure that:

- A whole-school safeguarding approach is taken to preventing harmful sexual behaviour
- All reports are taken seriously and responded to promptly
- Victims are supported, believed and protected
- Children displaying harmful behaviour receive appropriate safeguarding and educational support
- Incidents are managed in line with safeguarding and statutory procedures
- Patterns and trends are monitored to inform prevention strategies

Prevention and Education

The school will ensure that:

- High-quality Relationships and Sex Education (RSE) is delivered
- Learners are taught about consent, respectful relationships and healthy boundaries
- Online safety education addresses digital sexual abuse, coercion and image-based harm
- Sexist language, misogyny and harmful gender stereotypes are actively challenged
- Learners are encouraged to be positive bystanders and report issues they see
- Reporting systems are accessible, appropriate and clearly communicated

Reporting and Responding

The school will ensure that:

- Multiple reporting routes are available and understood
- All incidents are recorded securely in line with safeguarding and data security procedures
- Risk assessments are completed where appropriate
- The safety and wellbeing of those affected is prioritised
- External specialist agencies are involved where required
- Criminal matters are referred to the police where appropriate

Support and Risk Management

The school will ensure that:

- Victims receive appropriate pastoral and safeguarding support
- Children displaying harmful behaviour receive proportionate and educational intervention
- Risk assessments are dynamic and regularly reviewed
- Supervision and safety planning are proportionate and protective

Online Harmful Sexual Behaviour

Online incidents will be managed in line with national guidance and may involve specialist reporting services where appropriate.

Training and Review

The school will ensure that:

- DSPs receive specialist safeguarding training
- All staff receive regular safeguarding updates
- Governors receive appropriate oversight training
- This policy is reviewed annually and updated in response to legislative changes or emerging risks

Appendix A9 – Computer Misuse and Cyber Choices Policy Template

Purpose

The purpose of this policy is to set out the school's approach to preventing, identifying and responding to computer misuse and potential cybercrime involving learners.

Computer misuse is recognised as a safeguarding issue and this policy supports the school's wider safeguarding, Online Safety, Filtering and Monitoring, Technical Security and Cyber Security arrangements.

All key stakeholders, including the Local Authority and where applicable the Education Technology Support Partner, have responsibility for the safeguarding of young people from computer misuse and are aware of the Cyber Choices programme led by the National Crime Agency (NCA) and managed locally by Regional Organised Crime Units (part of the national policing network). The risks to young people of crossing the line into committing cybercrimes is a safeguarding issue.

This often happens without the individual realising their actions are criminal, which is why young people need support in making the right Cyber Choices in their use of technology. Young people with an interest in technology, a high IQ, and an appetite to engage in risky behaviours are considered to be at a higher risk of committing a cyber offence, but many first-time offenders are also unaware of what the law governing cyber offences actually is. The average age of first-time cyber offenders in the UK has fallen significantly in recent years. The Cyber Choices programme works with individuals committing, or at risk of committing, cybercrimes which can only be carried out with technology, where devices are both the tool for committing the crime, and the target of the crime.

Scope

This policy applies to:

- All learners, staff, volunteers and governors
- Behaviour occurring within and outside school where it impacts the school community

Policy Statement

The school will ensure that:

- Learners understand that some online activity is illegal
- Acceptable Use Agreements clearly outline legal expectations and consequences
- Computer misuse is treated as a safeguarding concern in the first instance
- Staff understand emerging cyber risks and referral routes
- Concerns are referred immediately to the Designated Safeguarding Person (DSP)
- Appropriate external advice or referral is sought where required

Prevention and Education

The school will ensure that:

- Learners are taught about the Computer Misuse Act 1990 and cybercrime risks
- Curriculum provision promotes ethical and lawful digital behaviour
- Online safety education addresses hacking, malware, phishing, denial-of-service activity and data misuse
- Learners are signposted to positive pathways for developing cyber skills
- Staff are aware of NCA Cyber Choices guidance and resources

Roles and Responsibilities

- Governors provide strategic oversight of safeguarding and cybercrime prevention.
- Senior Leaders ensure preventative education is delivered and staff are appropriately trained.
- The Designated Safeguarding Person (DSP) assesses concerns, completes safeguarding risk assessments, maintains records and seeks external advice where appropriate.
- Technical staff monitor network use in line with the Filtering and Monitoring Policy and report concerns to the DSP.
- All staff must report suspected computer misuse immediately and reinforce legal and ethical expectations.

Identification and Reporting

Computer misuse may include:

- Unauthorised access to systems or accounts
- Attempting to bypass filtering or monitoring controls
- Use of malware or hacking tools
- Denial-of-service activity
- Password harvesting or credential sharing
- Data theft or system interference

Where concerns arise, the matter will be referred to the DSP, a safeguarding risk assessment will be completed, and parents/carers will be informed unless doing so would increase risk.

Referral to Cyber Choices

Where the DSP believes that the learner may be at risk of committing cybercrimes, or to already be committing cybercrimes, a referral to the local Cyber Choices programme will be made (contact details for all Regional Organised Crime Units are available in the "what to do if you're concerned" section at the bottom of the NCA Cyber Choices page). Where the DSP is unsure if a learner meets the referral criteria, advice should be sought from the local Cyber Choices team:

- South Wales (incorporating South Wales Police, Gwent Police and Dyfed Powys Police force areas): tarian.cyber.prevent@south-wales.police.uk
- North Wales: Cyber.Prevent@nwrocu.police.uk

Parents and carers also have the opportunity report potential cybercrime directly to the local Cyber Choices team but are recommended to make school-based concerns through the DSP.

Support and Risk Management

The school will ensure that:

- Risk assessments are proportionate and regularly reviewed
- Educational and behavioural support is provided
- Learners are supported to redirect technical skills positively
- Safeguarding responses are consistent with the wider safeguarding framework

Training and Awareness

The school will ensure that:

- Staff receive safeguarding updates relating to computer misuse risks
- DSPs understand referral routes and thresholds
- Governors understand oversight responsibilities
- Parents/carers are signposted to relevant guidance where appropriate

Monitoring and Review

- This policy will be reviewed annually and updated in response to legislative changes, national guidance or emerging risks.
- Incident trends and safeguarding reviews will inform continuous improvement.

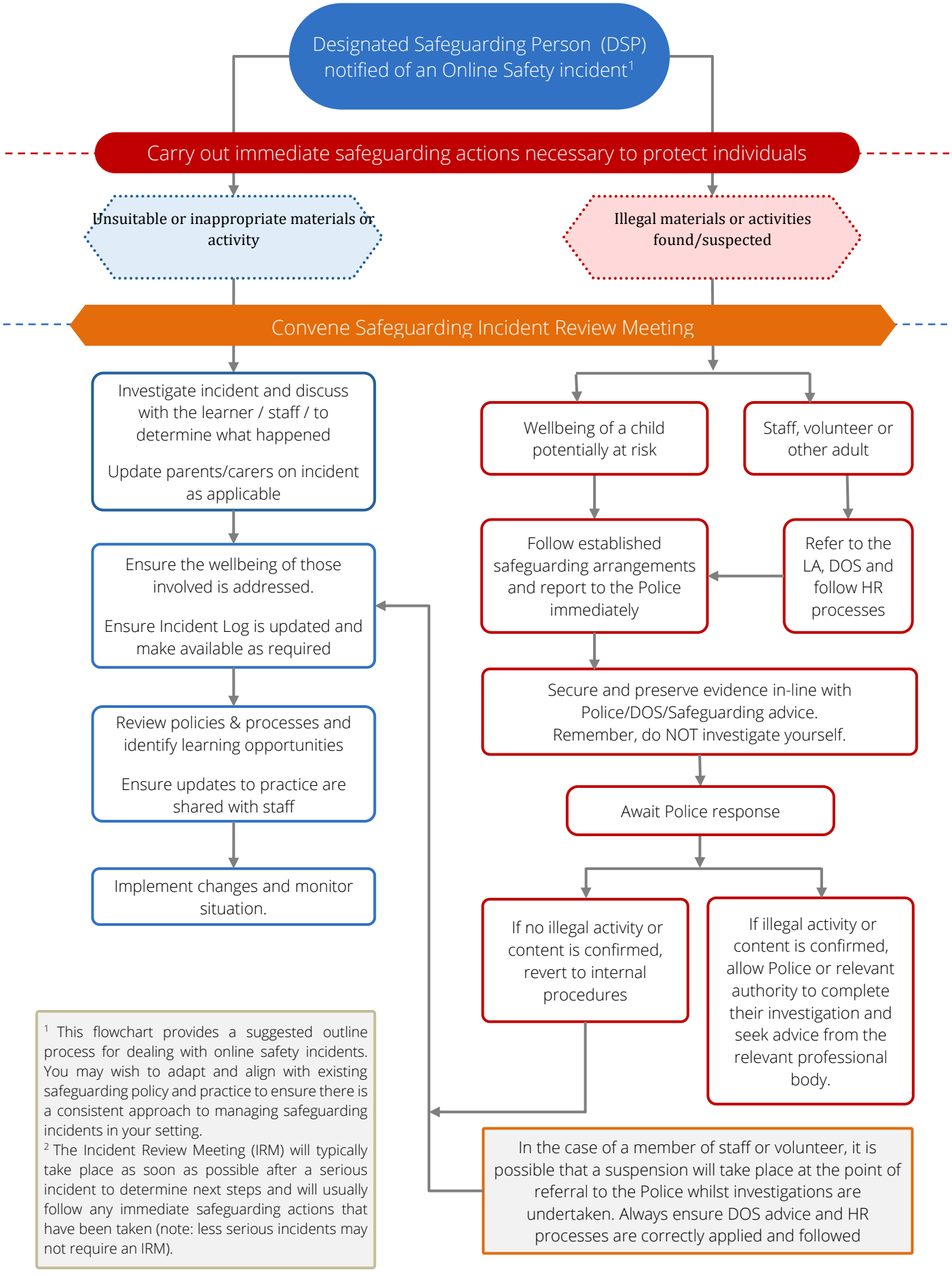
This policy template is based on a document for schools published by the South East Regional Organised Crime Unit (SEROCU) and has been amended for use across the UK. SWGfL would like to acknowledge the support of SEROCU for permission to adapt and use the document.

Schools will need to contact their local ROCU / Cyber Choices team regarding local processes:

North Wales - Cyber.Prevent@nwrocu.police.uk

Other regions - tarian.cyber.prevent@south-wales.police.uk.

Appendix A10 - Responding to incidents of misuse – flow chart



[1] This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.

[2] The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).

Appendix A11 - Record of reviewing devices/sites (responding to incidents)

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

Details of first reviewing person

Name: .....

Position: .....

Signature: .....

Details of second reviewing person

Name: .....

Position: .....

Signature: .....

Name and location of computer used for review (for web sites)

.....

.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

Appendix A12 - Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Appendix B1 - Training Needs Audit Log

Name / Group: .....

Relevant training in the last 12 months	Identified Training Need	To be met by	Cost	Review Date

Appendix C1 – Web Filtering and Online Safeguarding Policy Template

Purpose

- The purpose of this policy is to ensure that appropriate web filtering and online safeguarding systems are in place to safeguard learners and staff from harmful or illegal online content, while enabling safe and effective teaching, learning and professional practice. Web filtering and online safeguarding form part of the school's wider safeguarding responsibilities and are implemented in line with Keeping Learners Safe and the Education digital standards

Scope

This policy applies to:

- All users of the school's digital environment
- All school-owned devices
- Any device accessing the school's network or internet connection
- Web filtering and online safeguarding provided through third-party or managed services

Roles and Responsibilities

- Governors provide strategic oversight and assurance that web filtering and online safeguarding standards are met.
- Senior leaders ensure appropriate systems are in place, reviewed and resourced.
- The DSP/OSL lead safeguarding responses arising from web filtering and online safeguarding alerts.
- The IT service provider / Education Technology Support Partner maintains systems and provides reports as agreed.
- All staff report concerns relating to access, alerts or system effectiveness.

Policy Statement

The school will ensure that:

- Internet access is filtered to block illegal, harmful and inappropriate content
- Monitoring systems are in place to identify safeguarding concerns and enable timely intervention
- Web filtering and online safeguarding is proportionate, transparent and risk-based
- Roles and responsibilities are clearly defined and understood
- Provision is reviewed regularly and improved in response to risk, practice and guidance

Web filtering and online safeguarding are recognised as supporting safeguarding, not replacing education, supervision or professional judgement.

Filtering

The school will ensure that web filtering systems:

- Block access to illegal content, including child sexual abuse material, terrorist material and other unlawful content
- Manage inappropriate and/or harmful content (including search terms and results). These may include:
    - Gambling
    - Hate speech/discrimination
    - Harmful content
    - Mis/Disinformation
    - Piracy and copyright theft
    - Pornography
    - Self-harm and eating disorders
    - Violence against women and girls
- Are age-appropriate and suitable for an educational environment
- Are applied consistently to all users, devices and internet connections, including backup connections
- Allow the identification of individual users and devices in the event of breaches of the web filtering policy
- No user should be able to deactivate or bypass systems that filter illegal content.
- Prevent circumvention through VPNs, proxy services or similar technologies
- Support differentiated access for different user groups (e.g. staff and learners)
- Are reviewed regularly to avoid inappropriate over-blocking that may restrict teaching and learning

The school understands the capabilities and limitations of the system and potential impact on implementation and policy is understood.

The school will use recognised tools and guidance to assure the effectiveness of web filtering provision e.g., testfiltering.com

Online safeguarding

The school will ensure that online safeguarding:

- Enables the identification of safeguarding concerns in a timely manner
- Uses a combination of physical supervision, manual checks and technical systems as appropriate
- Generates alerts that can be prioritised and acted upon by trained staff
- Is subject to human review and professional judgement
- Is clearly communicated to users through policy and acceptable use agreements

Online safeguarding should be proportionate to the school's risk profile and should not create a culture of surveillance.

Review and Training

Web filtering and online safeguarding provision should be reviewed at least annually and whenever risks or technologies change. Staff, governors and those with specific responsibilities will receive appropriate training.

Appendix C2 - Technical Security Policy Template

(including Access, Device and Incident Management)

Purpose

- This policy sets out how the school protects its technical infrastructure, systems and devices to ensure a secure and resilient digital environment. It supports safeguarding, data protection and business continuity and aligns with the Education digital standards

Scope

This policy applies to:

- Staff, learners and governors
- Suppliers of third-party services and solutions
- School networks, servers and cloud systems
- School-owned devices
- User accounts and access controls
- Device configuration and management, including personal devices where permitted

Policy Statement

The school will ensure that its technical systems are managed in a way that:

- Protects users and data from unauthorised access or misuse
- Supports safe and reliable access to digital services
- Enables detection, response and recovery from technical incidents
- Is proportionate to risk and regularly reviewed

Access Control and Authentication

The school will ensure that:

- All users have unique accounts with appropriate access rights
- New user rights are allocated as part of induction
- Access is removed promptly when users leave the school
- Passwords and authentication methods reflect Cyber Essentials guidance and the Education digital standards
- Multi-factor authentication (MFA) is used for sensitive systems where appropriate
- Administrator access is restricted and monitored
- System administrators and those with global/ confidential data system access use a physical security device in addition to MFA to access systems.

System Security and Maintenance

The school will ensure that:

- Systems and software are licensed, supported and kept up to date
- Security patches are applied promptly
- Anti-virus and malware protection is in place across all systems
- Backups are taken regularly, stored securely (both locally and offsite, with rotation) and regularly tested
- Physical access to infrastructure is controlled

Device Management

The school will ensure that:

- The Device management standards are followed
- Clear expectations exist for the use of school-owned and personal devices
- School devices are configured securely and managed appropriately, with regular/ automatic patches and updates
- Where personal devices are permitted, expectations are clearly defined and risk-assessed
- Acceptable Use Agreements reference responsible device use
- Users receive guidance on safe and appropriate device use

Supplier Management

The school will ensure that:

- Provision of third-party services and solutions are adequately contracted and regularly reviewed
- Suppliers can demonstrate adherence to school policy and alignment with the Education digital standards

Incident Management

Technical incidents will be logged, escalated and reviewed. Serious incidents will be managed in line with safeguarding and business continuity procedures.

Review and Training

Technical security arrangements will be reviewed regularly. Staff with specific responsibilities will receive appropriate training, and users will be educated on their responsibilities.

Appendix C3 - Cyber Security Policy Template

Purpose

This policy sets out how the school prevents, detects, responds to and recovers from cyber threats. It supports the school's duty of care to protect users and data and aligns with the Education Digital Standards, Cyber response plan for schools, National Cyber Security Centre (NCSC) guidance and NCSC Cyber Essentials

Scope

This policy applies to:

- Cyber threats including phishing, ransomware, malware and unauthorised access
- Staff, learners and governors
- Suppliers of third-party services and solutions
- Technical systems and cloud services
- Incident response and business continuity

Policy Statement

The school will take a proactive, risk-based approach to cyber security to:

- Reduce the likelihood and impact of cyber incidents
- Ensure timely and effective response to threats
- Build awareness and resilience across the school community

Cyber Security Strategy

The school will maintain a cyber security strategy that:

- Is supported by senior leaders and governors
- Is informed by risk assessment and incident learning
- Is reviewed regularly in line with emerging threats
- Is inclusive of all services and solutions, including those from third-party suppliers

Supplier Management

The school will ensure that suppliers:

- Can demonstrate adherence to school policy and alignment with the Education digital standards and the Cyber response plan for schools,
- Are familiar with school incident response plan and able to respond effectively

Awareness and Education

The school will ensure that:

- Staff receive regular cyber-security training covering phishing, credential theft, malicious links, social engineering, ransomware, AI-enabled scams and other emerging threats.
- Learners receive age-appropriate education about cyber security, scams, account protection and the lawful and responsible use of systems.
- Governors understand their oversight responsibilities

Incident Response

The school will maintain a clear cyber incident response plan that:

- Defines roles and escalation routes
- Supported by an effective communications strategy
- Supports safeguarding and business continuity
- uses cyber incident exercises periodically to test preparedness and identify improvements.
- Ensures incidents are recorded and reviewed
- identifies responsibilities for safeguarding, technical response, communications, data protection and external reporting.

External Assurance

Where appropriate, the school will engage external expertise to assess cyber resilience and will work towards recognised standards or certifications.

Review

Cyber security arrangements will be reviewed annually, or sooner if required by incidents, guidance or changes in technology. Lessons learned from managing incidents should inform improvements to the strategy.

Appendix C4 - Data Security Policy Template

Purpose

The purpose of this policy is to ensure that personal and sensitive data is handled securely, lawfully and transparently, in line with UK data protection legislation and statutory guidance. The policy supports safeguarding, privacy, and trust across the school community and forms part of the school's wider approach to online safety and information security.

Scope

This policy applies to:

- All personal data processed by the school
- All staff, volunteers, governors and contractors
- Data subjects including staff, learners and parents/carers
- All digital and paper-based records
- All third parties processing data on behalf of the school

Legislative Context and guidance

The school complies with current UK data protection legislation, including UK GDPR as amended and supplemented by applicable UK legislation:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025, where relevant to the school's processing activities
- Freedom of Information Act
- Relevant guidance from the Information Commissioner's Office (ICO)
- Guidance for schools to implement the information management strategy
- Data protection for schools and colleges

Policy Statement

The school recognises its role as a Data Controller and is committed to ensuring that personal data is:

- Processed lawfully, fairly and transparently
- Collected for specified and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and kept up to date
- Retained only for as long as necessary
- Secured against unauthorised access, loss or misuse

Data security is recognised as a safeguarding responsibility and is embedded across leadership, governance and daily practice.

AI-enabled or automated systems involving personal data are assessed before use, including consideration of lawful basis, transparency, data minimisation, security, accuracy, bias and the need for human oversight.

Personal or sensitive information will only be entered into approved AI systems where the school's data protection and security requirements have been satisfied.

Governance and Roles

Data Protection Officer (DPO)

The school will appoint a Data Protection Officer (internal or external) who:

- Provides independent advice and monitoring of compliance
- Supports Data Protection Impact Assessments (DPIAs)
- Acts as the point of contact with the ICO
- Reports directly to senior leadership and governors

The DPO operates independently and is supported with appropriate time, access and resources.

Governors

Governors:

- Approve and review data protection policies
- Provide strategic oversight of compliance and risk
- Ensure adequate resources are allocated
- Receive reports on data breaches, audits and risks

Senior Leaders and Staff

Senior leaders ensure that:

- Data protection is embedded into systems and culture
- Staff receive appropriate training
- Procedures are implemented consistently
- Data breaches are managed in line with school policy and in accordance with ICO guidance

All staff and governors are responsible for handling personal data securely and reporting concerns or incidents promptly.

Lawful Processing and Transparency

The school will:

- Identify and document lawful bases for processing personal data
- Apply additional conditions for processing special category data
- Maintain clear and accessible Privacy Notices for learners, parents/carers, staff and governors
- Ensure data subjects understand their rights
- Ensure consent is considered and established with data subjects and used only where appropriate and never as a default where a public task or legal obligation applies.

Records, Mapping and Risk Management

The school will maintain:

- A Record of Processing Activities (RoPA)
- A data asset register, including third-party and cloud services
- Clear retention and disposal schedules
- Data Protection Impact Assessments (DPIAs) for new or high-risk processing

Data protection is considered at the design stage of any new system or process ("data protection by design and default").

Data Security and Access Controls

The school will ensure that:

- Access to personal data is role-based and restricted
- User accounts are protected by strong authentication
- Devices accessing personal data are secured and encrypted where appropriate
- Personal data is stored only on approved systems
- Cloud services meet UK data protection and security requirements
- Third-party contracts include appropriate data processing clauses
- Paper records are stored securely and disposed of appropriately.

Data Sharing and Transfer

Personal data will only be shared:

- Where there is a lawful basis
- With appropriate safeguards in place
- Using secure transfer methods
- With approved third parties

Additional care is taken when data is accessed remotely or transferred off-site.

Data Subject Rights

The school will uphold all data subject rights, including:

- Right to be informed
- Right of access (Subject Access Requests)
- Right to rectification
- Right to erasure (where applicable)
- Right to restrict or object to processing

Procedures are in place to manage requests within statutory timescales.

Data Breaches and Incident Management

The school will:

- Maintain clear procedures for reporting and managing data breaches
- Assess the risk to individuals' rights and freedoms
- Notify the ICO within 72 hours where required
- Record all breaches and near-misses
- Use learning from incidents to improve practice

Data breaches are treated as serious incidents and may also trigger safeguarding procedures where appropriate.

Training and Awareness

The school will ensure that:

- All staff and governors receive regular data protection training
- New staff receive training as part of induction
- Targeted training is provided where roles require it
- Learners are taught about privacy and data protection as part of the curriculum, in an age-appropriate way

Monitoring and Review

This policy will be:

- Reviewed at least annually
- Updated in response to changes in legislation, guidance or risk
- Supported by audits and compliance checks

Status

This Data Security Policy should be read alongside the school's:

- Safeguarding and Child Protection Policy
- Online Safety Policy
- Technical Security Policy
- Cyber Security Policy
- Records Management and Retention Policy

Appendix C5 – Public Online Communications Policy Template

Purpose

The purpose of this policy is to set out how the school manages public online communications in order to reduce risk, promote safeguarding and online safety, celebrate success and communicate effectively with the wider school community.

Public online communications include the school website, newsletters, learning platforms, public messaging systems and official social media accounts.

- This policy supports the Online Safety, Web Filtering and Online Safeguarding, Technical Security, Cyber Security and Data Security policies and reflects Keeping Learners Safe, Hwb – Policies, procedures, principals and practices for schools use of social media; Hwb Web Scraping (images) guidance.

Scope

This policy applies to:

- All staff and governors.
- All public online communications representing the school.
- Official school accounts and platforms.
- Personal accounts where their use directly references, represents or could reasonably be associated with the school in a professional context.
- School content published at any time, from any location or online platform.

Policy Statement

The school will ensure that:

- Public online communications are accurate, lawful and appropriate.
- Safeguarding considerations are prioritized.
- Personal data is protected in line with the Data Security Policy.
- Images and video are published only in line with consent procedures.
- Copyright and intellectual property are respected.
- Communications reflect professional standards.
- Public references to the school are monitored appropriately.
- Official public communications are made only through authorised school accounts and platforms.
- AI-generated or AI-assisted content is subject to appropriate human review and transparency labelling before publication.

Roles and Responsibilities

- Governors provide strategic oversight and assurance that public online communications meet safeguarding, data protection and statutory publication requirements.
- Senior leaders approve official accounts and oversee monitoring and moderation processes.
- Account administrators maintain secure access, monitor content regularly and ensure policy compliance.
- All staff must follow this policy, maintain professional standards and report concerns.

Creation of Public Online Accounts

- New public online accounts may only be created following approval by senior leadership.
- Proposals must define purpose, audience, responsible staff members and monitoring arrangements.
- At least two authorised staff members must have access to any official public account.
- Official accounts will be reviewed regularly and securely transferred, archived or closed when no longer required or when responsibility changes.

Monitoring and Moderation

The school will ensure that:

- Public communications are monitored regularly.
- Comments are reviewed and moderated appropriately.
- Monitoring of 'followers' of school accounts is undertaken regularly.
- Harmful or inappropriate content is addressed appropriately, including removal, reporting, preservation of evidence or escalation where necessary.
- Safeguarding concerns are reported immediately through the school's safeguarding procedures; other serious incidents are recorded and escalated to senior leaders or relevant external agencies as appropriate.

Professional Standards

All public communications must:

- Be respectful and professional.
- Avoid discriminatory, offensive or defamatory content.
- Protect confidentiality.
- Avoid internal grievance discussions.
- Avoid disclosure of sensitive information.

Use of Images and Media

- The school will ensure that:
- Appropriate consent is obtained.
- Images are appropriate and dignified.
- Learners are not identified unnecessarily.
- Images are removed where consent is withdrawn.
- To reduce the risk of images, video, audio or other content featuring staff or learners being copied, manipulated or misused, including through AI technologies, the school has procedures governing how such content is selected and shared publicly. (n.b. (e.g., UKSIC guidance Best Practices for Managing Images and Videos on School Websites, School Image Guidance, and Hwb Web Scraping (images) guidance.
- Staff consider whether location and context published alongside images could increase safeguarding or privacy risks.

Personal Use and Association with the School

Staff may use personal social media accounts; however:

- Where staff identify themselves as associated with the school, they must maintain appropriate professional boundaries and comply with relevant staff conduct and acceptable use expectations.
- Personal use must not impact professional standards nor school reputation.
- Staff must not engage with current learners via personal accounts.
- Excessive or inappropriate use during working hours may result in disciplinary action

Handling Complaints and Abuse

Where negative comments are made online:

- The school will respond proportionately.
- Abusive, threatening or harmful content will be managed proportionately, including recording, reporting, blocking, removal or referral to relevant platforms or agencies as appropriate.
- Parents/carers' complaints should be directed to formal complaints procedures.
- Serious matters may be escalated to senior leaders or external agencies.

Training and Awareness

The school will ensure that:

- Staff responsible for public accounts receive appropriate guidance and training on safeguarding, data protection, account security, moderation, escalation and the responsible use of AI-assisted content.

- Governors understand oversight responsibilities.
- The wider community is informed of expected standards.

Review and Continuous Improvement

This policy will be reviewed annually and updated in response to legislative changes, national guidance or emerging risks.

Appendix C6 - Generative Artificial Intelligence (gen AI) in Schools

Introduction

The South West Grid for Learning Trust (SWGfL) is a charity that has been at the forefront of supporting schools with online safety and security for 20 years and is recognised as a world leader in online safety innovation

As generative artificial intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of gen AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

Evidence is emerging about the benefits of gen AI to enhance personalised learning and streamline administrative tasks, while also raising concerns around data privacy, ethical use, and the preparedness of teachers to effectively integrate gen AI tools into classrooms.

This ongoing dialogue reflects the recognition of gen AI's transformative potential in education, balanced with a need for careful implementation to protect learner welfare and promote equitable outcomes. These considerations are shaping a pathway for embedding gen AI in schools, focusing on teacher training, ethical guidelines, and fostering digital competency among learners.

How to Use this Template

This document has been created as a template for school leaders to assist them in creating their own gen AI Policy.

Within this template, sections which include information or guidance are shown in BLUE. It is anticipated that schools would remove these sections from their completed policy document, though this will be a decision for the group that produces the policy.

Where sections in the template are written in ITALICS it is anticipated that schools would wish to consider whether to include that section or statement in their completed policy.

Legislative Background and Key Documents

The UK Online Safety Act 2023 is designed to make the internet safer, particularly for children and vulnerable users, by regulating online content and holding tech companies accountable

for harmful material. It is still yet to be fully understood where there may be gaps in regulation to protect children and young people from possible harm caused by AI. Ofcom is the online safety regulator in the UK and is responsible for publishing codes of practice and guidance on how companies can comply with their duties.

There is currently no specific legislation regarding the use of gen AI in schools, but guidance has been developed and is being regularly updated as the technology evolves. Schools may wish to consult the following resources:

- Generative artificial intelligence in education – opportunities and considerations for schools and settings
- Generative AI: Keeping learners safe online
- AI foundations online training module
- Hwb - What is artificial intelligence: video produced by the Wales Collaborative for learning design
- AI Opportunities Action Plan (UK Government)
- Ofcom's 2024 Online Nation Report
- EU Artificial Intelligence Act 2024 - Useful high-level 4-point summary of considerations
- UNESCO AI Competency Framework for Students (Guidance)
- UNESCO AI Competency Framework for Staff (Guidance)

Context

Gen AI represents a transformative leap in technology, enabling machines to create text, images, audio, and video with remarkable accuracy and creativity. Emerging from advancements in machine learning, particularly deep learning, generative models such as GPT (Generative Pre-trained Transformer) and DALL·E leverage vast datasets to understand and produce content that mimics human expression. Initially text-focused, these models have evolved to become multi-modal, integrating and processing various types of input, such as text and images, to generate cohesive outputs.

Since the debut of early systems like OpenAI's GPT-2 in 2019, the field has rapidly advanced, unlocking opportunities in education while raising critical considerations around ethics, data privacy, and equitable access.

According to Ofcom's 2025 Online Nation Report and the Ofcom 2025 Children and Parents Media Use and Attitudes Report generative AI adoption is significantly higher among children and teenagers than adults, with 79% of online teenagers (13–17) and 40% of younger children (7–12) using these tools. Snapchat My AI is the most popular platform, used by 51% of online youth aged 7–17, while ChatGPT is the leading tool for adults. Children use generative AI primarily for creative tasks, chatting, and finding

information, with 11% of 8–17-year-olds using AI as a conversational partner or "friend." However, there is a notable gap between confidence and competence: 40% of 13–17-year-olds trust AI-generated news as much as human-written content, and 25% of those claiming to spot AI-generated content failed to identify it when tested.

Schools must now navigate this landscape thoughtfully, crafting policies that harness the benefits of gen AI for creativity and learning while prioritising learners' safety, security and well-being.

Policy on the use of Gen AI in Schools

Statement of intent

Artificial Intelligence (AI) technology is already widely used in commercial environments and is gaining greater use in education. We recognise that integrating gen AI tools into education presents many opportunities, including the potential to enhance educational experiences and support staff with some administrative tasks. However, their use must prioritise safety, responsibility, ethics, trust and inclusivity.

We also realise that there are risks involved in the use of gen AI systems, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address risks.

We will educate staff and learners about safe and ethical use of gen AI, preparing them for a future in which AI technologies are likely to play an increasing role.

The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

Related policies

This policy should be read in conjunction with other school policies:

- Data Protection Policy
- Staff Discipline policies and codes of conduct
- Behaviour policy
- Anti-bullying policy
- Online safety policy
- Acceptable Use Agreements
- *Curriculum Policies*
- Add any other polices that may be relevant

Policy Statements

- The school acknowledges the potential benefits of the use of gen AI in an educational context - including enhancing learning and teaching, improving administrative processes, managing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use gen AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Learners Safe
- We will provide relevant training for staff *and governors* in the advantages, use of and potential risks of gen AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- We will seek to embed learning about gen AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with gen AI tools.
- As set out in the staff acceptable use agreement, staff will be supported to engage with gen AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff will only input anonymised data to avoid the exposure of personally identifiable or sensitive information.
- Staff will always ensure gen AI tools used comply with GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
- All staff will be required to carefully consider the use of any gen AI tool and involve senior leadership in decision-making around its use.
- Staff should always use school-provided accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party gen AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.
- The school will ensure that when gen AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train gen AI models without appropriate consent.
- Staff must report any incidents involving gen AI misuse, data breaches or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.

- The school will keep a record of all tools in use, their purpose and potential risks. (Risk assessment matrices are attached as an appendix)
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When acquiring and implementing gen AI systems, we will follow due care and diligence to prioritise fairness and safety.
- *The school will support parents and carers in their understanding of the use of gen AI in the school (this could be through an "AI in our school guide")*
- *Where staff use gen AI tools to support their learning and teaching practice, such as in the assessment of learners' work, this will be purposeful, considered, with a clear focus on ensuring impact and understanding and mitigating risk.*
- *Staff will ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance.*
- *Staff will ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing.*
- Improper use of gen AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

Responsibilities

Headteacher and Senior Leaders

Are responsible for the strategic planning of how gen AI will be used in the school, establishing AI policies and procedures and ensuring that all staff receive relevant training and have a clear understanding of these.

Designated Safeguarding Person (DSP) / Online Safety Lead

Our Designated Safeguarding Person / Online Safety Lead has responsibility for online safety in the school. They are expected to have knowledge of gen AI and its safeguarding implications and an in-depth working knowledge of key guidance. We ensure that they receive appropriate specialist training, commensurate with their role and that ongoing training is provided for all school staff.

Data Protection Officer

The DPO will be responsible for providing advice and guidance about data protection obligations in relation to the use of gen AI, including related Data Protection Impact Assessments (DPIAs).

Technical Staff

Technical staff / IT Leads will be responsible for technical support and guidance, with particular regard to cyber-security and the effectiveness of filtering and monitoring systems.

(Schools that have external contracts for technical support must ensure that their Education Technology Support Partner is aware of the school's requirements regarding gen AI and comply with school policies. Such schools should also audit these services for compliance)

Staff

It is the responsibility of all staff to have read and understood this policy and associated Acceptable Use Agreements. All staff must report any incidents or suspected incidents concerning the use of gen AI in line with school policy. All staff will challenge any inappropriate behaviour. Staff have a duty to ensure that:

- the school environment is safe
- sensitive and confidential data / information is secure
- that their actions do not put the reputation of the school at risk and that
- learners understand their responsibilities

Governors

We ensure that our governing body has a good understanding of how gen AI is used in a school context and potential benefits and risks of its use. They receive regular training and updates, enabling them to support the school and challenge where necessary. This may include evaluation of the use of gen AI in the curriculum, administration and communications, ensuring that risks relating to these issues are identified, that reporting routes are available, and that risks are effectively mitigated. (Schools may wish to add here any specific Governor committee that will take lead responsibility e.g., Risk and Audit Committee)

Parents/carers

We work hard to engage parents and carers by:

- *regular in school sessions*
- *sharing newsletters*
- *sharing information online e.g., website, social media*
- *providing curriculum information*
- List any other ways you may engage parents and carers

Our parents and carers are made aware of how gen AI is used in school and receive guidance on both good practice in its use and the risks of misuse that may affect their child's learning or safety. They are encouraged to report any concerns to the school and are made aware that all incidents will be handled with care and sensitivity.

Vulnerable groups

We recognise that vulnerable learners are more likely to be at risk from the misuse of gen AI (both in their own use or through the actions of others). We ensure that vulnerable learners

are offered appropriate support to allow them to gain full benefit of the use of gen AI, while being aware of the potential risks.

Children are considered vulnerable data subjects and therefore any process involving their personal data is likely to be "high risk". If an AI automated process is used to make significant decisions about people, this is likely to trigger the need for a Data Protection Impact Assessment (DPIA).

Reporting

Our reporting systems are well promoted, easily understood and easily accessible for staff, learners and parents/carers to confidently report issues and concerns, knowing these will be treated seriously. All reports will be dealt with swiftly and sensitively and outcomes shared where appropriate. We also respond to anonymous reports, or reports made by third parties. This can be done via: (amend as necessary)

- nominated member of staff
- established school reporting mechanisms
- online/offline reporting tool
- anonymous/confidential reporting routes
- links to national or local organisations
- *list any other systems here*

Responding to an incident or disclosure

Our response is always based on sound safeguarding principles and follows school safeguarding and disciplinary processes. It is calm, considered and appropriate and puts the learner at the centre of all decisions made.

- All gen AI incidents (including data breaches and/or inappropriate outputs) must be reported promptly to the relevant internal teams. Effective reporting helps mitigate risks and facilitates a prompt response.
- Where relevant / required incidents will be reported to external agencies e.g., Police, local authority, Data Protection Officers, ICO.
- All AI related incidents will be recorded through the school's normal recording systems

In the case of misuse of gen AI by staff, the normal staff disciplinary processes will be followed.

Risk assessment

It is key that our approach to managing risk aligns with, and complements, our broader safeguarding approach.

The school understands that despite many positive benefits in the use of gen AI, there are some risks that will need to be identified and managed, including:

- Legal, commercial, security and ethical risks
- Data Protection
- Cyber Security
- Fraud
- Safeguarding and well-being
- Duty of care

The example matrix included at the end of this policy template may be used to evaluate risk within the school and may be edited and adapted accordingly through the normal school procedures

Education and training

Our school's educational approach seeks to develop knowledge and understanding of emerging digital technologies, including gen AI.

This policy outlines our commitment to integrating gen AI effectively within our school environment. We will use gen AI responsibly, safely and purposefully to support with a variety of tasks such as:

- assisting with some routine administrative functions
- helping provide more personalised learning experiences
- supporting lesson planning, marking, feedback and reporting
- providing contexts to support development of critical thinking skills
- supporting school-level curriculum and assessment design

AI literacy, which includes being able to think critically, engage with evidence and information, verify sources and use creativity, will be fundamental. The skills integral to the four purposes, which should be developed across all Areas of Learning and Experience in the Curriculum for Wales, are focused on building these dispositions. Our school's approach is to deliver this knowledge and understanding where it is appropriate and relevant in our curriculum.

Our approach is given the time it deserves and is authentic i.e., based on current issues nationally, locally and within our setting's risk profile. It is shaped and evaluated by learners and other members of the school community to ensure that it is dynamic, evolving and based on need. We do this by:

- *Engaging with learners*

- *Critical evaluation of emerging trends and research findings*
- *Surveys*
- *Focus groups*
- *Parental engagement*
- *Staff consultation*
- *Staff training*

As gen AI becomes an integral part of modern education, it is important that staff develop the knowledge and skills to integrate gen AI tools responsibly into teaching, learning, and administrative processes. By fostering AI literacy, staff can confidently prepare learners for a future where AI is a key driver of innovation and opportunity.

- We will support and ensure all staff can access training on the effective, responsible, and ethical use of emerging technologies in education.
- We will integrate AI-related risks and safeguards into annual safeguarding training, aligning with statutory guidance, including 'Keeping Learners Safe'.
- We will support staff to identify, assess, and mitigate risks associated with gen AI technologies, including issues such as biased algorithms, privacy breaches, and harmful content.
- We will support staff to ensure compliance with UK GDPR and other relevant regulations while using gen AI systems.
- We will promote ethical practices in the use of gen AI, ensuring that these technologies contribute to equity, fairness, and inclusivity in education.
- We will empower staff to teach learners about the safe and ethical use of gen AI, cultivating a culture of awareness, resilience, and informed decision-making in the digital age.

The following resources are used:

- Generative AI – Hwb guidance - Resources, guidance and information for education practitioners, learners, and families on generative AI.
- Hwb - Sharing nudes and semi-nudes: Responding to incidents and safeguarding children and young people
- Common Sense Education AI literacy and digital citizenship materials
- Curriculum for Wales - Hwb
- AI Foundations: training module for education practitioners

Additional links

- SWGfL – Artificial Intelligence and Online Safety

Appendix C6a - Risk Assessment Matrix for Schools Implementing gen AI

Introduction

The following risk assessment matrix is intended to help schools identify, evaluate, and mitigate risks associated with implementing gen AI in educational processes.

The matrix considers potential risks across various domains, including data protection, ethical considerations, and operational integrity. There is a particular focus on safeguarding and wellbeing issues, highlighting potential risks to learner welfare and offers strategies to mitigate these risks effectively. Schools should amend the content of the matrix as necessary and consider the risk profile that is relevant to their own circumstances.

Risk Assessment Matrix

Risk Area	Risk Description	Likelihood (Low/Med/High)	Impact (Low/Med/High)	Risk Level (Low/Med/High)	Mitigation Measures
Gen AI training	Insufficient training or guidance impacting the ability of staff to adopt, use, and monitor gen AI safely and ethically within their school.				Ensure all staff can access regular training to support the safe and ethical use of gen AI in teaching and learning.
Data Protection and Privacy Breaches	Unauthorised access to sensitive data or personal information, leading to safeguarding concerns and commercial risk.				Implement strong encryption, regular audits, and GDPR-compliant data management policies and conduct regular privacy audits.
Cyberbullying	Increased potential for bullying through AI-mediated communication tools.				Monitor gen AI communication tools, implement clear reporting mechanisms, and provide learner support.
Over-reliance on gen AI	Over-reliance on gen AI tools reducing				Encourage collaborative

	interpersonal interactions among learners. Reduction in teacher autonomy and critical decision-making by overusing gen AI tools.				learning activities and balance gen AI use with social engagement. Define clear boundaries for gen AI use and regularly review its impact on pedagogy.
Emotional Manipulation	Gen AI systems unintentionally affecting learner mental health through curated content.				Monitor AI-generated content, involve mental health professionals, and promote media literacy.
Inappropriate Content or Conduct	Gen AI exposing learners to harmful or unsuitable materials / behaviour				Conduct rigorous testing of gen AI tools, apply effective filtering and monitoring and ensure human oversight.
Mental Health Impacts	Overuse of gen AI tools causing stress, anxiety, or dependency in learners.				Monitor usage patterns, provide mental health resources, and set expectations on use of gen AI systems.
Bias and Discrimination	Gen AI systems propagating biases that impact learner wellbeing or inclusion. Gen AI models producing discriminatory or biased outcomes.				Regularly audit gen AI algorithms for bias and provide inclusive media literacy education and training.
Misuse of AI	Learners using gen AI tools for harmful, unethical or illegal				Educate learners on responsible and appropriate gen AI

	purposes (e.g. nudification).				use and establish clear usage policies.
Misinformation	Creation or spread of harmful or misleading AI-generated content.				Educate staff and learners to verify gen AI outputs and establish clear policies for verifying content authenticity.
Digital Divide	Inequitable access to gen AI tools among learners from diverse demographic groups.				Provide equitable access to gen AI resources and ensure alternative solutions are available.
AI Ethics Awareness	Lack of awareness among staff and learners about ethical implications of gen AI.				Provide training and education on gen AI ethics and its responsible usage. Establish an 'Ethics in AI' group.
Data Accuracy	Gen AI systems generating inaccurate or misleading recommendations.				Regularly validate gen AI outputs and involve human oversight in decision-making.
Legal Compliance	Non-compliance with laws regarding gen AI usage and learner data.				Understand legal requirements. Conduct legal reviews and consult experts on gen AI-related regulations.
Cyber-Security	Increased use of gen AI tools in cyberattacks targeting school systems and data.				Strengthen cybersecurity protocols and educate staff and

					learners on safe online practices.

Likelihood and Impact Definitions

- Likelihood: The likelihood that the identified risk will occur.
    - Low: Unlikely to occur under normal circumstances.
    - Medium: Possible occurrence based on past trends or vulnerabilities.
    - High: Likely to occur without intervention.
- Impact: The severity of impact should the risk materialise.
    - Low: Minimal disruption with limited consequences.
    - Medium: Moderate disruption affecting key processes.
    - High: Significant disruption with severe consequences.

Action Plan

Schools may wish to create an action plan based on the findings of the risk assessment matrix. Your plan should consider a before and after approach to demonstrate the intended impact of your proposed actions. These actions might include (amend as relevant).

1. *Appoint a safeguarding lead to oversee gen AI implementation and its impact on learner welfare.*
2. *Deliver regular training for staff on online safety, AI ethics, and responsible use.*
3. *Review curriculum offer to identify where gen AI-related issues might be incorporated into learning in relevant and appropriate parts of the curriculum.*
4. *Establish transparent reporting mechanisms for any safeguarding or wellbeing concerns linked to gen AI.*
5. *Collaborate with parents and carers to raise awareness about gen AI risks and best practices.*
6. *Conduct annual reviews of gen AI tools and their impact on learner wellbeing, updating the risk matrix as needed.*

Review and Update

The school will review and update this matrix annually or whenever new AI technologies or safeguarding challenges arise.

Appendix C6b - GenAI and Emerging Technologies Staff (and Volunteer) Acceptable Use Agreement

It will be for schools to decide if they wish to have a specific Gen AI Staff/Volunteer Acceptable Use agreement as provided below or whether to rely on the references within the general Staff/Volunteer AUA (as in Appendix A4)

School Policy

Emerging technologies, including gen AI, are increasingly integrated into educational settings and the lives of staff and learners. These technologies have potential to enhance creativity, promote personalised learning, and improve operational efficiency. However, their use also presents risks that require clear policies and practices to ensure safety, security, and ethical application.

This acceptable use policy aims to ensure:

- Staff and volunteers are responsible users of gen AI and emerging technologies, prioritising safety and ethical considerations.
- School systems and users are protected from misuse or harm resulting from the use of gen AI.
- Staff have a clear understanding of their responsibilities when engaging with gen AI and emerging technologies in professional and personal contexts.

Acceptable Use Agreement

I understand that I must use gen AI and emerging technologies responsibly to minimise the risk to the safety, privacy, or security of the school community and its systems. I acknowledge the potential of these technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos and values.

For my professional and personal safety:

- I understand that the school will monitor my use of gen AI tools and technologies.

- I will only use gen AI tools and technologies for purposes authorised by the school and will ensure compliance with data protection laws (e.g. UK GDPR) when handling personal data.
- I will ensure that any sensitive or personally identifiable information about staff, learners, or parents/carers is only entered into gen AI systems that have explicit approval and robust security measures in place.
- I will report any gen AI-related incidents or anomalies that could indicate misuse, bias, or harm to the appropriate person immediately.

In my communications and actions:

- I will respect copyright, intellectual property, and ethical standards when uploading content to prompt gen AI outputs.
- I will critically evaluate the outputs of gen AI systems to avoid spreading misinformation or biased content and will ensure that all AI-assisted decisions are made with appropriate human oversight.
- I will communicate professionally and responsibly when using gen AI systems.
- I will ensure transparency through appropriate attribution where gen AI has been used.

When engaging with learners:

- I will support learners on the safe, ethical, appropriate and effective use of gen AI.
- I will use gen AI tools to engage with learners in ways that uphold and enhance their privacy, wellbeing, and trust.

When using the school's systems and resources:

- I will use gen AI systems in compliance with established security measures and access protocols.
- I will ensure that any gen AI applications used in teaching or administration are vetted and comply with the school's policies.
- I will ensure gen AI tools are not used to impersonate others or create deceptive or harmful content.

When handling data:

- I will ensure compliance with the school's data protection policies when using gen AI for data analysis or reporting.
- I will ensure I have explicit authorisation when uploading sensitive school-related information into gen AI systems.

Responsibility and Accountability:

- I will use gen AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identities and well-being.
- I understand that misuse of gen AI or emerging technologies could lead to disciplinary actions, including warnings, suspension, or referral to the appropriate authorities.
- I acknowledge that this agreement applies to all gen AI-related activities within and outside of school premises that are connected to my professional responsibilities.

Appendix C6c - Gen AI Tools Request Form

It is recommended that schools only allow the use of Gen AI tools which have been approved by the school. The form below allows staff to seek approval for the use of tools which they have found to be useful and are likely to meet the school's approval criteria.

Contact person:

Position:

Date of request:

Gen AI Tool/Resource Details

Name of AI tool/resource:

Purpose of use:

Expected benefits:

Potential risks:

The following points have been acknowledged: (please circle – YES / NO)

- GDPR UK compliance: Users of Gen AI must uphold their data protection responsibilities in accordance with the General Data Protection Regulation (GDPR UK).

- Acceptable use agreement: Users of Gen AI must ensure that its use is consistent with the school's Staff Acceptable Use Agreement and should understand their responsibilities for mitigating associated risks, as outlined here: https://hwb.gov.wales/support-centre/education-digital-standards/generative-artificial-intelligence-in-education#considerations-for-schools-and-settings-around-generative-ai

- Gen AI use case: Users must establish a clear purpose for deploying and using specific Gen AI tools through effective and ethical use.

adteacher Approval: (please circle – YES / NO)

Date of approval:

Acknowledgement: This form is derived from one used by Bridgend Council for its schools.

Legislation

Schools should be aware of the legislative framework under which this online safety policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

A useful summary of relevant legislation can be found at: Report Harmful Content: Laws about harmful behaviours

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Schools may wish to view the National Crime Agency website which includes information about the Cyber Choices programme. The TARIAN Regional Cyber Crime Unit (RCCU) now has dedicated 'Cyber Prevent' officers whose role is to prevent young people from committing cybercrime and/or re-offending. Supportive resources are available on Hwb.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

The Data Protection Act 2018:

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

The Data (Use and Access) Act 2025 (DUAA)

Updates, rather than replaces, existing UK data protection law, including UK GDPR and the Data Protection Act 2018. For schools, the fundamental requirements to handle personal data lawfully, fairly, transparently and securely remain, but the Act introduces and clarifies provisions relating to areas such as lawful processing, automated decision-making, data sharing and the handling of data protection complaints. Schools should review their data protection policies, privacy information and procedures to ensure they reflect the changes, paying particular attention to how pupil, staff and parent/carer data is collected, accessed, shared and used, and to the use of emerging technologies and online services that process personal data.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities

have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly

- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the Revenge Porn Helpline

Online Safety Act 2023

The Online Safety Act 2023 is a new set of laws that protects children and adults online. It puts a range of new duties on social media companies and search services, making them more responsible for their users' safety on their platforms. The Act will give providers new duties to implement systems and processes to reduce risks their services are used for illegal activity, and to take down illegal content when it does appear.

Ofcom is the independent regulator of Online Safety. It will set out steps providers can take to fulfil their safety duties in codes of practice. It has a broad range of powers to assess and enforce providers' compliance with the framework.

Protections for young people

The Online Safety Act creates a legal responsibility (a "duty of care") for the operators of user-to-user services to protect users under the age of 18 from harmful content, specifically

- Enforcing minimum age requirements
- Publishing risk assessments
- Protecting children from harmful content published on the service
- Properly applying the Terms and Conditions

Protections for adults

While the Act focusses on the need to protect young people online, there are some provisions that focus on protecting adults (which will benefit all users) including

- Ability to customise your feed
- Block online trolls
- Criminalising certain content
- Remove content that is already illegal

Enforcement

Ofcom has been appointed as the regulator and have powers to obtain information from website operators on how they deal with online harms and to take action if they fail to comply with their new duties, including

- Investigate website operators and their compliance with the Bill
- Issue financial penalties to companies that do not comply with their obligations
- Issue guidance on compliance
- Issue notices requiring website operators to give information or cooperate with an Ofcom investigation

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

Welsh Government

Safeguarding children (including Keeping Learners Safe)
School bullying advice

Hwb

Hwb homepage
Online safety: Five key questions for governing bodies to help challenge their schools and colleges to effectively safeguard their learners
Digital Competence Framework
Health and Well-being AOLE
Keeping Learners Safe Modules 4 and 5 Online Safety for Practitioners and Governors
Delivering online learning: safeguarding principles and practice
Safer Internet Day resources
Advice for schools on preparing for and responding to viral online harmful challenges and hoaxes
Practices and principles for schools' use of social media
Keeping safe online
Hwb Trust Centre
Education Digital Standards

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Revenge Porn Helpline - https://revengepornhelpline.org.uk/
Internet Watch Foundation - https://www.iwf.org.uk/
Report Harmful Content - https://reportharmfulcontent.com/
Harmful Sexual Support Service

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

Kent – Online Safety Resources page
INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/

UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Tools / Resources for Schools / other organisations

SWGfL Test filtering - http://testfiltering.com/

Childline – Report / Remove

SWGfL- Assisted Monitoring

SWGfL – Resources for Education

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Childnet – Cyberbullying guidance and practical PSHE toolkit:
http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit

Childnet – Project deSHAME – Online Sexual Harrassment

UKSIC – Sexting Resources

Ditch the Label – Online Bullying Charity

Diana Award – Anti-Bullying Campaign

Social Networking

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Hwb - Web scraping

Hwb Keeping safe online - App guides for families

Hwb Keeping safe online - social media

Hwb - Practices and principles for schools' use of social media

Hwb - Responding to online reputational issues and harassment directed at schools and school staff

Data Protection

Welsh Government - Guidance for schools to implement the information management strategy

Hwb School Data Sharing Agreement

Hwb - Data protection for schools and colleges

Hwb – Data protection posters

ICO Guides for Organisations

ICO Guidance on taking photos in schools

Professional Standards/Staff Training

DCF Professional Learning Needs Tool

UK Safer Internet Centre Professionals Online Safety Helpline

SWGfL – Online Safety Training

Infrastructure/Technical Support/Cyber-security

Education Digital Standards

Hwb Cyber Response Plan for Schools

Hwb Cyber security in schools: questions for governing bodies...
Cyber Resilience Centre for Wales
Tarian – What is cyber-crime?
UKSIC – Appropriate Filtering and Monitoring
SWGfL Safety & Security Resources
SWGfL - Cyber Security in Schools.
NCA – Guide to the Computer Misuse Act

Working with parents and carers

Hwb – App guides for families
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops/education
Internet Matters

Prevent

Prevent Duty Guidance
Childnet – Trust Me

Research

Ofcom – Childrens Media Habits

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in August 2026. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.

© SWGfL 2026