Hywel Dda Primary School
Online Safety Policy
September 2025

Version Control:

Version	Last Modified	Last Modified By	Document Changes	Date presented to and agreed by Governing Body
1	July 2025	James Jones	Full update	

UNCRC:

16. Protection of privacy

Every child has the right to privacy. The law must protect children's privacy, family, home, communications and reputation (or good name) from any attack.

17. Access to information

Children have the right to get information from the Internet, radio, television, newspapers, books and other sources. Adults should make sure the information they are getting is not harmful. Governments should encourage the media to share information from lots of different sources, in languages that all children can understand.

<u>**Online Safety Policy**</u>

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 devices on the school site (where allowed).

Date created: [27/06/25]

Next review date: [26/06/26]

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Hywel Dda Primary School to safeguard members of our school community online in accordance with principles of open government and with the law.

This Online Safety 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 devices on the school site (where allowed).

Hywel Dda Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Policy development, monitoring and review

This Online Safety Policy has been developed by the staff and Governors, including:

• headteacher/senior leaders

• online safety lead

• staff – including teachers/education practitioners/support staff/technical staff

• governors

• parents and carers

• community users

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for development, monitoring and review

This Online Safety Policy was approved by the *school governing body on:*	2nd July 2025
The implementation of this Online Safety Policy will be monitored by:	Online Safety Lead – James Jones
Monitoring will take place at regular intervals:	Each summer term
The *governing body* will receive a report on the implementation of the Online Safety Policy at regular intervals:	Each summer term
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	June 2026

Should serious online safety incidents take place, the following external persons/agencies should be informed, as necessary	• Chair of Governors • LA ICT manager, • LA safeguarding officer, • Police

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

•   logs of reported incidents

•   monitoring logs of internet activity

•   internal monitoring data for network activity

•   surveys/questionnaires of:

o   learners

o   parents and carers

o   staff

Policy and leadership

Responsibilities

In order to ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

Headteacher and senior leaders

•   The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to an appropriate member of the middle leadership team.

•   The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

•   The headteacher/senior leaders are responsible for ensuring that all staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.

• The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.

• The headteacher/senior leaders will receive regular monitoring reports from the Online Safety Lead.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the Welsh Government and UKCIS document Five key questions for governing bodies to help challenge their school to effectively safeguard their learners. This will be carried out by the (insert name of governor group/committee) whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

• regular meetings with the Online Safety Lead

• regularly receiving (collated and anonymised) reports of online safety incidents

• checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)

• reporting to relevant governors group/meeting

• membership of the school Online Safety Group

• occasional review of the filtering change control logs and the monitoring of filtering logs (where possible)

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Online Safety Lead

The Online Safety Lead will:

• lead the Online Safety Group

• work closely on a day-to-day basis with the Designated Safeguarding Persons (DSPs), where these roles are not combined

• take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns

• have a leading role in establishing and reviewing the school online safety policies/documents

• promote an awareness of and commitment to online safety education across the school and beyond

• liaise with curriculum leaders to ensure that the online safety curriculum is planned and embedded

• ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents

- receive reports of online safety incidents and create a log of incidents to inform future online safety developments

- provide (or identify sources of) training and advice for staff/ governors/ parents/ carers/ learners

- liaise with (school/local authority) technical staff, pastoral staff and support staff (as relevant)

- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs

- attend relevant governing body meetings/groups

- report regularly to headteacher/senior leadership team

- liaises with the local authority/relevant body

Designated Safeguarding Persons (DSPs)

The Designated Safeguarding Person should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data

- access to illegal/inappropriate materials

- inappropriate online contact with adults/strangers

- potential or actual incidents of grooming

- online bullying

Curriculum Leads

Curriculum Leads will work with the online safety lead to develop a planned and coordinated online safety education programme. This will be provided through:

- a discrete programme

- the Digital Competence Framework

- relationships and sexuality education

- Health and Wellbeing area of learning and experience

- assemblies and pastoral programmes

•	through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

<u>Teaching and support staff</u>

School staff are responsible for ensuring that:

•	they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices

•	they understand that online safety is a core part of safeguarding

•	they have read, understood and signed the staff acceptable use agreement (AUA), and that this is reviewed regularly

•	they follow all relevant guidance and legislation including, for example, Keeping Learners Safe and UK GDPR regulations

•	they immediately report any suspected misuse or problem to Karen Flynn, Lead DSP and Headteacher, for investigation/action, in line with the school safeguarding procedures

•	all digital communications with learners, parents and carers and others should be on a professional level and only carried out using official school systems and devices (where staff use Generative AI, they should only use school-approved Generative AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements

•	online safety issues are embedded in all aspects of the curriculum and other activities

•	ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

•	they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies with regard to these devices

•	in lessons where internet use is pre-planned learners should be guided to sites that are checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

•	where lessons take place using live-streaming or video-conferencing, staff must have full regard to Live-streaming and video-conferencing: safeguarding principles and practice guidance, which outlines key considerations to ensure safe practice when live-streaming.

•	they adhere to the school's technical security policy, with regard to the use of devices, systems and passwords and understand basic cybersecurity

•	they have a general understanding of how the learners in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies

• they are aware of the benefits and risks of the use of Generative Artificial Intelligence (GenAI) services in school, being transparent in how they use these services, prioritising human oversight. Gen AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

• they have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc

• they model safe, responsible and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Network manager/technical staff

The network manager/technical staff (or local authority/managed service provider) is responsible for ensuring that:

• they are aware of and follow the school Online Safety Policy and Technical Security Policy in order to carry out their work effectively in line with school policy

• the school technical infrastructure is secure and is not open to misuse or malicious attack

• the school meets (as a minimum) the required online safety technical requirements as identified by the local authority, Welsh government via the Education Digital Standards or other relevant body

• users may only access the networks and devices through a properly enforced password protection policy

• they keep up-to-date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

• the use of the technical and communications systems is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Lead for investigation and action

• monitoring software/systems are implemented and updated as agreed in school or education technology support partner policies

Learners

• are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and this is reviewed annually

• should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

• should know what to do if they or someone they know feels vulnerable when using online technology

• should avoid plagiarism and uphold copyright regulations, taking care when using Generative Artificial Intelligence (GenAI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through gen AI services.

- will be expected to know and follow school Online Safety Policy

- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

The school will take every opportunity to help parents and carers understand these issues through:

- providing them with a copy of the learners' acceptable use agreement

- publish information about appropriate use of social media relating to posts concerning the school

- seeking their permissions concerning digital images, cloud services etc

- providing opportunities for parents and carers to improve their understanding of online safety through parents'/carers' evenings, newsletters, letters, website, Hwb, learning platform and information about national/local online safety campaigns and literature

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school

- the use of their children's personal devices in the school

Community users

Community users who access school systems/website/Hwb/learning platforms as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems.

Professional Standards

There is an expectation that national professional standards will be applied to online safety as in other aspects of school life i.e.

- there is a consistent emphasis on the central importance of literacy, numeracy, digital competence and digital resilience. Learners will be supported in gaining skills across all areas of learning and every opportunity will be taken to extend learners' skills and competence

- there is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience, while taking care to avoid risks that may be attached to the adoption of developing technologies e.g. Generative Artificial Intelligence (GenAI) tools.

- practitioners are able to reflect on their practice, individually and collectively, against nationally agreed standards of effective practice and affirm and celebrate their successes

• policies and protocols are in place for the use of online communication technology be-tween the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

• Where Generative AI is used to monitor staff communications, it will be balanced with respect for privacy and transparency about what is being monitored and why

Policy

Online Safety Policy

The school Online Safety Policy:

• sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication

• allocates responsibilities for the delivery of the policy

• is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours

• establishes guidance for staff in how they can use digital technologies responsibly, protecting themselves and the school and how they can use this understanding to help safeguard learners in the digital world

• describes how the school will help prepare learners to be safe and responsible users of online technologies

• establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms

• is supplemented by a series of related acceptable use agreements

• is made available to staff at induction and through normal communication channels

• is published on the school website

Acceptable use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable use agreements

The Online Safety Policy and appendices define acceptable use at the school. Within the appendices there are acceptable use agreements for:

- learners – differentiated by age. Learners will be introduced to the acceptable use rules at induction, the start of each school year and regularly re-enforced during lessons, assemblies and by posters/splash screens around the school. Learner groups (to be described) are encouraged to suggest child friendly versions of the rules.

- staff /volunteer AUAs will be agreed and signed by staff and volunteers

- parent/carer AUAs inform them of the expectations of acceptable use for their children and seek permissions for digital images, the use of cloud systems etc.

- community users that access school digital technology systems will be required to sign an AUA

The acceptable use agreements will be communicated/re-enforced through:

- staff induction and handbook

- digital signage

- posters/notices around where technology is used

- communication with parents/carers

- built into education sessions

- school website

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Any illegal activity for example: • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	• Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering N.B. Schools should refer to guidance about dealing with self-generated nude and semi-nude images (sometimes referred to as 'sexting') - Sharing nudes and semi-nudes: Responding to incidents and safeguarding children and young people.					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) N.B. Schools will need to decide whether these					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways – read more about this: NCA Cyber Choices Programme					
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)				X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
	Infringing copyright and intellectual property (including through the use of Generative AI services)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

	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 permission/ awareness
Online gaming (not gambling)			X					X
Online shopping/commerce			X		X			
File sharing			X		X			
Social media			X		X			
Messaging/chat			X		X			
Entertainment streaming e.g. Netflix, Disney+			X		X			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok			X		X			
Mobile phones may be brought to school		X						X
Use of mobile phones for learning at school		X			X			
Use of mobile phones in social time at school		X			X			
Taking photos on mobile phones/cameras				X				X

Use of other personal devices, e.g. tablets, gaming devices			X					X
Use of personal email in school, or on school network/wi-fi			X		X			
Use of school email for personal emails	X				X			
Use of gen AI services that have not been approved by the school/LA/WG	X				X			

When using communication technologies, the school considers the following as good practice:

• when communicating in a professional capacity, staff should ensure that the communication tools they use are officially sanctioned by the school

• any digital communication between staff and learners or parents/carers (email, Class DOJO, social media, learning platform, etc.) must be professional in tone and content.

• staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community

• users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication

Reporting and responding

The school has in place procedures for identifying and reporting cases, or suspected cases, of online safeguarding issues/incidents and understands that because of our day-to-day contact with children our staff are well placed to observe the outward signs of these issues.
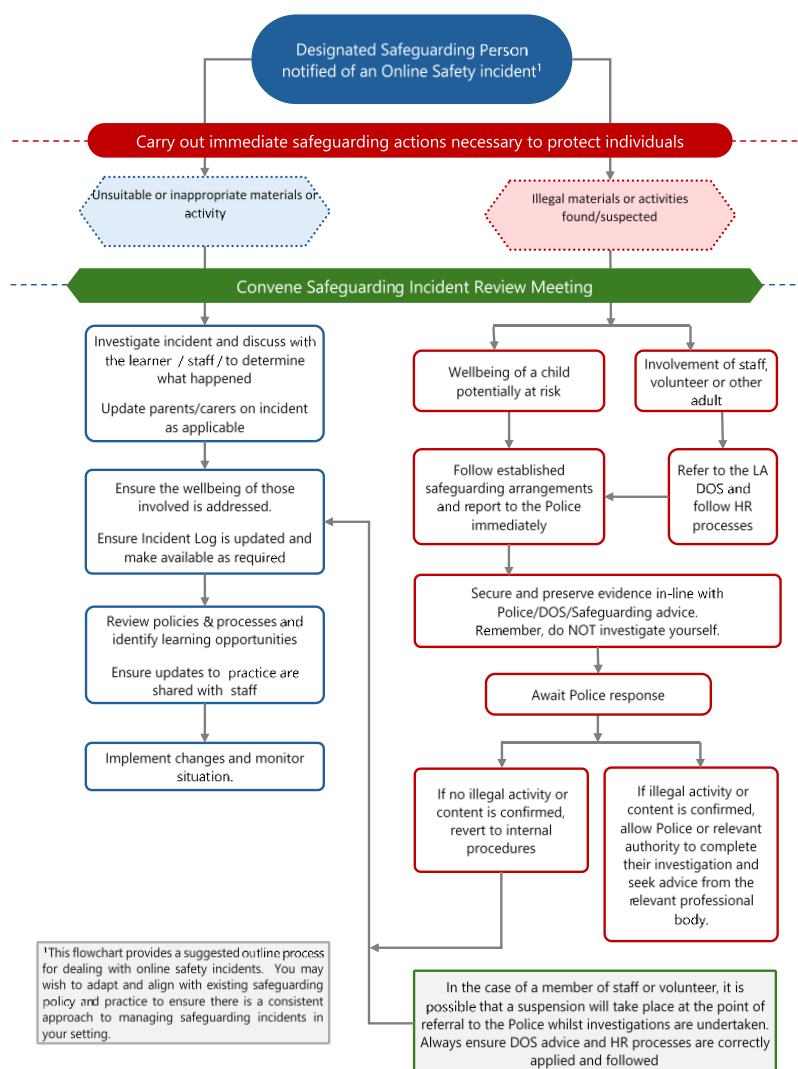
We ensure that every member of staff and every governor knows that they have an individual responsibility for reporting and that they are aware of the need to be alert to signs of abuse and neglect and know how to respond to a learner who may disclose such issues.

We also understand that reporting systems do not always respond to the needs of learners and that we need to identify issues and intervene early to better protect learners.

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

•   there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.

•   all members of the school community will be made aware of the need to immediately report online safety issues/incidents

•   reports will be dealt with as soon as is practically possible once they are received

•   the Designated Safeguarding Person, Online Safety Lead and other responsible staff have appropriate skills and training to deal with the various risks related to online safety

•   if there is any suspicion that the incident involves child abuse images, any other illegal activity or the potential for serious harm, the incident must be escalated through the normal school safeguarding procedures and the police informed. In these circumstances any device involved should be isolated to support a potential police investigation.
In addition to child abuse images such incidents would include:

•   incidents of 'grooming' behaviour

•   the sending of obscene materials to a child

•   adult material which potentially breaches the Obscene Publications Act

•   criminally racist material

•   promotion of terrorism or extremism

•   other criminal conduct, activity or materials.

•   any concern about staff misuse will be reported immediately to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority

Designated Safeguarding Person notified of an Online Safety incident[1]

Carry out immediate safeguarding actions necessary to protect individuals

Unsuitable or inappropriate materials or activity

Illegal materials or activities found/suspected

Convene Safeguarding Incident Review Meeting

Investigate incident and discuss with the learner / staff / to determine what happened
Update parents/carers on incident as applicable

Ensure the wellbeing of those involved is addressed.
Ensure Incident Log is updated and make available as required

Review policies & processes and identify learning opportunities
Ensure updates to practice are shared with staff

Implement changes and monitor situation.

Wellbeing of a child potentially at risk

Involvement of staff, volunteer or other adult

Follow established safeguarding arrangements and report to the Police immediately

Refer to the LA DOS and follow HR processes

Secure and preserve evidence in-line with Police/DOS/Safeguarding advice. Remember, do NOT investigate yourself.

Await Police response

If no illegal activity or content is confirmed, revert to internal procedures

If illegal activity or content is confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.

[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.

In the case of a member of staff or volunteer, it is possible that a suspension will take place at the point of referral to the Police whilst investigations are undertaken. Always ensure DOS advice and HR processes are correctly applied and followed

The school will make the flowchart above available to staff to support the decision-making process for dealing with online safety incidents.

<u>School actions</u>

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

<u>Responding to Learner Actions</u>

Incidents	Refer to class teacher/tutor	Refer to Head of Department / Principal Teacher / Deputy Head	Refer to Headteacher	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/ network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X	X		X	X	X	
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords			X						
Corrupting or destroying the data of other users.						X	X	X	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X				X	X	X	X
Unauthorised downloading or uploading of files or use of file sharing.	X							X	
Using proxy sites or other means to subvert the school's filtering system.					X				

15

Incidents								
Accidentally accessing offensive or pornographic material and failing to report the incident.						X	X	
Deliberately accessing or trying to access offensive or pornographic material.		X		X		X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.		X			X	X			
Unauthorised use of digital devices (including taking images)	X	X				X	X		
Unauthorised use of online services	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	X
Continued infringements of the above, following previous warnings or sanctions.		X	X			X	X	X	X

Responding to Staff Actions

Incidents	Refer to line manager	Refer to Headteacher/ Principal	Refer to local authority/MAT/HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		**X**	**X**	**X**				

Actions which breach data protection or network / cyber-security rules.	X				X		
Deliberately accessing or trying to access offensive or pornographic material.	X	X	X			X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.	X	X				X	X
Using proxy sites or other means to subvert the school's filtering system.	X		X			X	X
Unauthorised downloading or uploading of files or file sharing.	X	X	X			X	X
Breaching copyright / intellectual property or licensing regulations (including through the use of Generative AI services)	X	X				X	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature.	X	X			X		
Using personal email/social networking/messaging to carry out digital communications with learners and parents/carers	X				X	X	X
Inappropriate personal use of the digital technologies e.g. social media / personal email.	X	X			X	X	X
Careless use of personal / sensitive data, e.g. displaying, holding or transferring data in an insecure manner.	X	X			X		X
Actions which could compromise the staff member's professional standing.	X	X			X	X	X

Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.								
Failing to report incidents whether caused by deliberate or accidental actions.	X					X	X	X
Continued infringements of the above, following previous warnings or sanctions.	X						X	X

<u>The use of Generative Artificial Intelligence (GenAI) systems in School</u>

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, data protection 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.

<u>Policy Statements</u>

Only Microsoft Co-pilot will be used in schools in Wales, accessed via Hwb.

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 potential 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 always ensure gen AI tools used comply with UK GDPR and other data protection regulations, verifying with the Data Protection Officer (DPO) that tools com-ply with standards set by the Information Commissioner's Office (ICO) 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. Schools and practitioners will not input any personal data, learner data or other sensitive or confidential information into gen AI tools.

• 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.

• The school will keep a record of all tools in use, their purpose and potential risks.

• 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

• Where staff use gen AI tools to support their learning and teaching practice, this will be purposeful, considered, with a clear focus on ensuring impact and understanding and mitigating risk.

• 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.

Education

Online Safety Education Programme

While regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's safeguarding provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways.

The Citizenship Strand of the DCF will lead the progression in teaching the skills and knowledge needed for online safety.

• a planned online safety curriculum across all year groups and a range of subjects, (e.g. DCF/PSE/RSE/Health and Well-being) and topic areas and should be regularly revisited

• key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities

• it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week

• the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language. Learners considered to be at increased risk online (e.g. children in care, ALN learners, learners experiencing loss or trauma or mental health issues) are provided with targeted or differentiated online safety education

• learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information (including where the information is gained from Gen AI services)

• learners should be taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of Gen AI services

• learners should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

• learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school

• staff should act as good role models in their use of digital technologies the internet and mobile devices

• in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

• where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites/ tools (including Gen AI systems) the learners visit

• it is accepted that from time to time, for good educational reasons, learners may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff (or other nominated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

• the online safety education programme will be regularly audited and evaluated to ensure the quality of learning and outcomes.

Contribution of Learners

How safe do learners feel? The United Nations Convention on the Rights of the Child (UNCRC) sets out that "children have a right to be safe and protected from harm, and have the right to express their opinions and participate in decision-making."

In accordance with the UNCRC, the best way to understand how safe an education setting feels to learners is to ask them and observe how they and staff interact.

The school acknowledges, learns from and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

• mechanisms to canvass learner feedback and opinion.

• appointment of digital leaders and anti-bullying ambassadors within our pupil councils

• learners contribute to the online safety education programme e.g. digital leaders leading lessons for younger learners, online safety campaigns, Safer Internet Day events

• learners designing/updating acceptable use agreements

• contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

Staff/volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

• a planned programme of formal online safety, cyber security and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. It is expected that some staff will identify online safety as a training need within the performance management process

• the training will be an integral part of the school's annual safeguarding / data protection and cyber-security training for all staff

• all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours

• The Designated Safeguarding Person (or other nominated person) will receive regular updates through attendance at external training events, (e.g. Hwb Keeping safe online training events, from the Regional Consortium/SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations

- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days

- the Online Safety Lead will provide advice/guidance/training to individuals as required.

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in a number of ways such as:

- Hwb training – Online safety for governors

- attendance at training provided by the local authority

- participation in school training/information sessions for staff or parents

A higher level of training will be made available to (at least) the Online Safety Governor and should include training on filtering and monitoring systems used by the school, data protection, cyber-security and new developments in digital technologies.

Families

The school will seek to provide information and awareness to parents and carers through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes

- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops/parent/carer evenings etc

- the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.

- letters, newsletters, website, learning platform, Hwb

- high profile events/campaigns e.g. Safer Internet Day

- reference to the relevant web sites/publications, e.g. Hwb Keeping safe online, The UK Safer Internet Centre, Childnet International (see Appendix for further links/resources).

- Sharing good practice with other schools in clusters and or the local authority

Adults and Agencies

The Enhancing digital resilience in education: An action plan to protect children and young people online draws upon the self-review information schools in Wales record in the 360 safe Cymru tool. This data highlights that schools showing the strongest performance, amongst other indicators.

Drawing on this intelligence, the school will provide opportunities for local community groups and members of the wider community to gain from the school's online safety knowledge and experience. This may be offered through the following:

•   providing family learning courses in use of new digital technologies and online safety

•   online safety messages targeted towards families and relatives.

•   the school will provide online safety information via their learning platform, website, and social media for the wider community

•   supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision

The school recognises the support and advice that may be provided by external groups and agencies and values their contribution to school programmes and events.

The school is committed to sharing its good practice with other schools and education settings.

Technology

The school is responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures that are in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Filtering

•   the school filtering policies are agreed by senior leaders and technical staff and systems are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents and behaviours

•   the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the Welsh Government Education Digital Standards - Web filtering and the UK Safer Internet Centre Appropriate filtering. (The school will need to decide on the merits of external/internal provision of the filtering service – see Technical Security Policy Template in the Appendix).

•   internet access is filtered for all users

•   illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated

•   there are established and effective routes for users to report inappropriate content and this is acted upon in a timely manner by the Designated Safeguarding Person whilst adhering to the Wales Safeguarding Procedures

•   there is a clear process in place to deal with requests for filtering changes (see Appendix for more details).

•   the school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users: staff/learners, etc.)

•   younger learners will use child friendly/age-appropriate search engines e.g. Google safe search, SWGfL Swiggle

•   there is an appropriate and balanced approach to providing access to online content according to role and/or need

•   filtering logs are reviewed frequently and alert the school to breaches of the filtering policy, which are then acted upon. Devices that are provided by the school have school-based filtering applied irrespective of their location.

•   where personal mobile devices are permitted for use, there is clear separation between the school network filtering and the associated guest network filtering.

•   the system manages access to content through non-browser services (e.g. apps and other mobile technologies)

If necessary, the school will seek advice from, and report issues to, the Report Harmful Content site.

<u>Monitoring</u>

The school monitors network traffic at a local level, follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through:

•   the school monitoring policies are agreed by senior leaders and technical staff and systems are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents and behaviours

•   a staff lead who is responsible for managing the monitoring strategy and processes.

•   physical monitoring (adult supervision in the classroom)

•   internet use is logged, regularly monitored and reviewed

•   monitoring and filtering logs are regularly analysed and breaches are reported to senior leaders

•   Devices that are provided by the school have school-based monitoring applied irrespective of their location.

•   monitoring enables alerts to be matched to users and devices.

•   there is a clear process for prioritising response to alerts that require rapid safeguarding intervention.

•   management of serious safeguarding alerts is consistent with safeguarding policy and practice.

•   where Gen AI –supported monitoring is used, the purpose and scope of this is clearly communicated

•   pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.

• where possible, school technical staff regularly monitor and record the activity of users on the school technical systems

Users are made aware, through the acceptable use agreements, that monitoring takes place.

<u>Technical Security</u>

The school has a clear technical security policy and systems will be managed in ways that ensure- that the school meets recommended technical requirements

• system security training is available for all staff users

• there will be regular reviews and audits of the safety and security of school technical systems and of the school's technical support

• servers, wireless systems and cabling are securely located and physical access restricted

• there are rigorous and verified back-up routines, including the keeping of copies off-site or in the cloud and these are resilient by design

• A documented access control model should be in place, clearly defining access rights to school systems and devices. This should be reviewed annually. all users (staff and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Sharing of passwords or username and passwords could lead to an offence under the Computer Misuse Act 1990. Users must immediately report any suspicion or evidence that there has been a breach of security

• all school networks and systems will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password

• the master account passwords for the school systems are kept in a secure place, e.g. school safe.

• systems are in place for the recovery and resetting of passwords

• passwords should be long

• Only if necessary, records of learner usernames and passwords for Foundation Phase learners may be kept in an electronic or paper-based form, but they must be securely stored when not required by the user

• password requirements for learners at Year 3 and above should increase as learners progress through school

• the Online Safety Lead, with the support of the LA's technical support team, is responsible for ensuring that software licence logs are accurate and up-to-date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

• an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)

- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc., from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

- systems and programme software are regularly updated with security patches

- an agreed policy is in place for the provision of temporary access of 'guests', (e.g. trainee teachers, supply teachers, visitors) onto the school systems

- an agreed policy is in place regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school devices that may be used out of school

- an agreed device management policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices

- an agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices.

- systems are in place that prevent the unauthorised sharing of personal / sensitive data unless safely encrypted or otherwise secured. Care should be taken when using Gen AI services to avoid the input of sensitive information, such as personal data, internal documents or strategic plans, into third-party Gen AI systems unless explicitly vetted for that purpose. Staff must always recognise and safeguard sensitive data.

- encryption is used for the transfer of sensitive or vulnerable data and on school managed devices

- dual-factor authentication is used for sensitive data or access outside of a trusted net-work

- where Gen AI systems are used for technical security, their effectiveness is regularly re-viewed, updated and monitored for vulnerabilities.

- where Gen AI systems are used, the school will work with suppliers to understand how these services are trained and will regularly review flagged incidents to ensure equality for all users e.g. avoiding bias

Devices

- The school acceptable use agreements for staff, learners, parents and carers outline the expectations around the use of devices.

The school allows:

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device e.g. LA staff	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes – at times and with permissio	Yes	Yes

				ns		
Full network access	Yes	Yes	Yes	No	No	No
Internet only				Yes – at times and with permissions	Yes – at times and with permissions	Yes
No network access						

School owned devices:

• to whom they will be allocated

• where, when and how their use is allowed – times/places/in/out of school

• if personal use is allowed

• levels of access to networks/internet (as above)

• management of devices/installation of apps/changing of settings/monitoring

• network/broadband capacity

• technical support

• filtering of devices

• access to cloud services

• use on trips/events away from school

• data protection

• taking/storage/use of images

• exit processes, what happens to devices/software/apps/stored data if user leaves the school

• liability for damage

• staff training.

Personal devices

• which users are allowed to use personal mobile devices in school (staff/learners/visitors)

• restrictions on where, when and how they may be used in school

• if used in support of learning, how staff will plan their lessons around the potential variety of device models and different operating systems

- storage

- whether staff will be allowed to use personal devices for school business

- levels of access to networks/internet (e.g. access, or not, to internet/guest wi-fi/network)

- network/broadband capacity

- technical support

- filtering of the internet connection to these devices and monitoring the access

- management of software licences for personally owned devices

- data protection

- taking/storage/use of images

- liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility)

- identification/labelling of personal devices

- how visitors will be informed about school requirements

- how education about the safe and responsible use of mobile devices is included in the school online safety education programmes

- how misuse will be dealt with

Social media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published
- providing education/training on social media use including; acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
- having in place clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk
- provision of guidance for learners, parents/carers

School staff ensure that:

- no reference is made in social media to learners, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions are not attributed to the school or local authority

- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of social media

When official school social media accounts are established, there will be:

- a process for approval by senior leaders
- clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- personal communications which do not refer to or impact upon the school are outside the scope of this policy
- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- the school permits reasonable and appropriate access to private social media sites

Monitoring of public social media

- As part of active social media engagement, the school will pro-actively monitor the Internet for public postings about the school
- the school will effectively respond to social media comments made by others according to a defined policy or process
- when parents/carers express concerns about the school on social media, we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.
- If posts on social media by parents/staff are specifically unkind or malicious, or aimed at individual staff members, the Head will arrange to meet with these parents/carers and find a suitable way forward, including requests to remove the offending posts.

School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

Digital and video images

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- should a maintained school or setting choose to use live-streaming or video-conferencing, governing bodies, headteachers and staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the Live-streaming and video-conferencing: safeguarding principles and practice guidance and Keeping Learners Safe para 7.6
- when using digital images, staff should inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, e.g. on social networking sites
- 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 is 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
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images. Staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes

• care should be taken when taking digital/video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute

• learners must not take, use, share, publish or distribute images of others without their permission

• photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images

• learners' full names will not be used anywhere on a website or blog, particularly in association with photographs

• written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. Permission is not required for images taken solely for internal purposes.

In the event that one parent gives permission and one explicitly refuses permission, then we will not use photographs of that child. We will seek legal advice and advice from other relevant parties if needed.

• parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school Data Protection Policy

- images will be securely stored on the school network in line with the school retention policy and in accordance with the Data Protection Act 2018

• learners' work can only be published with the permission of the learner

Online safety messaging

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website

- o Social media
- o Class DOJO App
- o Online newsletters
- o Other

The school website is managed/hosted by Juniper (formerly PrimarySite). The school ensures that good practice has been observed in the use of online publishing e.g. use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is no risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected and full names are not published.

The school public online publishing provides information about online safety e.g. publishing the schools Online Safety Policy; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process

Data Security

• has a Data Protection Policy.

• implements the data protection principles and can demonstrate that it does so

• has paid the appropriate fee to the Information Commissioner's Office (ICO)

• has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.

• has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it

• the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed

• has an Information Asset Register (IAR) in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it

• the IAR lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed

• will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this

• data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals

•   provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)

•   has procedures in place to deal with the individual rights of the data subject. For example, one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them

•   carries out Data Protection Impact Assessments (DPIAs) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier

•   IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners

•   has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors

•   understands how to share data lawfully and safely with other relevant data controllers. In Wales, schools should consider using the Wales Accord on Sharing Personal Information (WASPI) toolkit to support regular data sharing between data controllers

•   has clear and understood policies and routines for the deletion and disposal of data

•   reports any relevant breaches to the Information Commissioner within 72 hours of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. To do this it has a policy for reporting, logging, managing, investigating and learning from information risk incidents

•   as a maintained school, has a Freedom of Information Policy which sets out how it will deal with FOI requests

•   provides protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

•   ensures that where Gen AI services are used, data privacy is prioritised

When personal data is stored on any mobile device or removable media the:

•   data will be encrypted and password protected.

•   device will be password protected.

•   device will be protected by up to date virus and malware checking software

•   data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

• at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse

• can recognise a possible breach, understand the need for urgency and know who to report it to within the school

• can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school

• only use encrypted mobile devices (including USBs) for personal data, particularly when it is about children

• will not transfer any school personal data to personal devices. Procedures should be in place to enable staff to work from home (i.e. VPN access to the school network, or a work laptop provided).

• use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

• transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

Cyber Security

Enhancing digital resilience in education: An action plan to protect children and young people online describes cyber security as:

"The term used to describe how both individuals and organisations can reduce the risk of cyber attacks. Cyber security's main purpose is to ensure the technology we use (devices such as computers, tablets and smartphones) and the services we access online are protected from the risk posed by cyber crime including theft for gain such as ransomware attacks and seeking competitive advantage, or malicious damage intended to disrupt an organisation's ability to operate effectively. We store large amounts of personal and organisational information on devices and services and preventing unauthorised access to this information is critical."

The 'Cyber security in schools: questions for governing bodies and management committees' guidance produced by the National Cyber Security Centre (NCSC) working with Welsh Government aims to support governing bodies' and management committees' understanding of their education settings' cyber security risks. The guidance includes eight questions to facilitate the cyber security conversation between the governing body and school leaders, with the governing body taking the lead.

The school may wish to consider the following statements, amending them in the light of their current cybersecurity policy, processes and procedures:

• the school has adopted and made use of the relevant Hwb Network and Data Security Standards

• the school, in partnership with their education technology support partner, has identified the most critical parts of the school's digital and technology services and sought assurance about their cyber security

- the school, in partnership with their education technology support partner, has an effective backup and restoration plan in place in the event of cyber attacks

- the school's governance and IT policies reflect the importance of good cyber security

- staff receive training on the common cyber security threats and incidents that schools experience the school has a business continuity and incident management plan in place that includes IT and these wider services.

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g. online safety education, awareness and training

- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors

- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising

- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate

- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.