



ONLINE SAFETY POLICY

Version Control	Version 1
Adoption Date	14 th July 2025
Review Date	Summer 2027

Chair of Governors		14 th July 2025
Headteacher		14 th July 2025



CONTENTS

Our Purpose, Vision and Values	3
1. Introduction.....	4
2. Responsibilities.....	5
3. Professional standards	10
4. Policy	10
5. Acceptable use	11
6. Reporting and responding.....	13
7. School actions.....	17
8. The use of Generative Artificial Intelligence (GenAI) systems in school.....	21
9. Education.....	23
10. Technology	27
11. Filtering.....	27
12. Monitoring.....	28
13. Technical security.....	29
14. Devices.....	31
15. Social media.....	36
16. Digital and video images	37
17. Online safety messaging.....	38
18. Data security.....	39
19. Cyber security.....	41
20. Outcomes	42
Appendix A: Learner Acceptable Use Agreement - Lower School Pupils.....	43
Appendix B: Learner Acceptable Use Agreement - Middle and Upper School Pupils.....	44
Appendix C: Acceptable Use Agreement - Staff and Visitors	46



OUR PURPOSE, VISION AND VALUES

PURPOSE

At Ysgol Bro Taf we are committed to harnessing the power of education to enrich our learners' lives, ensuring that the communities of Pontypridd thrive now and for future generations.

Delivering equity and excellence is at the heart of our school, where there is a place and opportunity for everyone, every day, to discover their brilliance.

VISION

- Foster a culture of aspiration where everyone strives to discover their brilliance
- Provide a dynamic and innovative curriculum which broadens our learners' horizons through progressive learning experiences
- Enable consistently outstanding teaching and embrace every moment as an opportunity to learn
- Build **ONE** community characterised by fun, equity, and inclusivity, where everyone feels supported, trusted and valued
- Empower our community to realise that leadership is not confined to a select few but can be embraced by all.

VALUES

Be Brave	We will not be afraid to take risks and will overcome challenges by being resilient.
Be Respectful	We will be kind and value everyone in our community.
Be Optimistic	We will embrace opportunities and challenges with a 'can-do' attitude.
Be Trusting	We will rely on each other's integrity and competence, fostering a collaborative and supportive culture.
Be Aspirational	We will set ambitious goals, strive for excellence and pursue personal growth to achieve our full potential.
Have Fun	We will promote enjoyment and seek fulfilment, celebrating both our individual and collective achievements.

1. INTRODUCTION

- 1.1. This Online Safety Policy outlines the commitment of Ysgol Bro Taf to safeguard members of our school community online in accordance with principles of open government and with the law.
- 1.2. This Online Safety Policy applies to all members of the school community (including staff, pupils, 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).
- 1.3. Ysgol Bro Taf 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.

2. RESPONSIBILITIES

- 2.1. 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

- 2.2. 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 senior leadership team.
- 2.3. The Headteacher and Assistant Headteacher (Progress and Digital Transformation) 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.
- 2.4. The Headteacher and 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.
- 2.5. The Headteacher and 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.
- 2.6. The Headteacher and senior leaders will receive regular monitoring reports from the Online Safety Lead.

Governors

- 2.7. 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 Online Safety Group 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)*

- 2.8. 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 - Assistant Headteacher (Progress and Digital Transformation)

- 2.9. The online safety lead will:
- lead the Online Safety Group
 - work closely on a day-to-day basis with the Designated Safeguarding Person (DSP), 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 Person (DSP)

- 2.10. 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.

Head of Lower School, Head of Faculty and Heads of AoLE

- 2.11. Curriculum Leads will work with the online safety lead to develop a planned and coordinated online safety education programme. This will be provided through (amend/delete as relevant):
- a discrete programme
 - the Digital Competence Framework

- relationships and sexuality education
- Health and Well-being area of learning and experience
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff

2.12. 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 Assistant Headteacher (Progress and Digital Transformation) 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 have an understanding of 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.

ExtraScope

2.13. ExtraScope 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 Assistant Headteacher (Progress and Digital Transformation) for investigation and action
- the [filtering policy](#), is applied and updated on a regular basis by the Local Authority
- monitoring software/systems are implemented and updated as agreed in school or education technology support partner policies.

Learners

2.14. 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

- 2.15. 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
- 2.16. 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 (where this is allowed)

Community users

- 2.17. 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.
- 2.18. The school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

Online Safety Group

- 2.19. The Online Safety Group has the following members:
- Online Safety Lead - Assistant Headteacher (Progress and Digital Transformation)
 - Designated Safeguarding Person
 - Online safety governor
 - ExtraScope technical staff.
- 2.20. Members of the Online Safety Group will assist the Online Safety Lead with:
- the production/review/monitoring of the school Online Safety Policy/documents
 - the production/review/monitoring of the school web filtering policy and requests for filtering changes
 - mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage of the Digital Competence Framework
 - reviewing network/web filtering/monitoring/incident logs, where possible
 - encouraging the contribution of learners to staff awareness, recent trends and the school online safety provision
 - consulting stakeholders – including staff/parents/carers about the online safety provision

- monitoring improvement actions identified through use of the 360 degree safe Cymru self-review tool.

3. 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 between 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.

4. 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.

5. ACCEPTABLE USE

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

Acceptable use agreements

- 5.2. An Acceptable Use Agreement is a document that outlines a school's expectations on the responsible use of technology by its users. In most schools they are signed or acknowledged by their staff as part of their conditions of employment. Some may also require learners and parents/carers to sign them, though it is more important for these to be understood and followed rather than just signed.
- 5.3. 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
 - staff /volunteer AUAs will be agreed and signed by staff and volunteers
 - parent/carers 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.
- 5.4. The acceptable use agreements will be communicated / re-enforced through:
- splash screens
 - digital signage
 - posters / notices around where technology is used
 - communication with parents and 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:	<p>Any illegal activity for example:</p> <ul style="list-style-type: none"> • Child sexual abuse imagery*s • 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 • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering. 					✓
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	<ul style="list-style-type: none"> • 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) 					✓
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)			✓	✓	
	Promotion of any kind of discrimination				✓	
	Using school systems to run a private business				✓	
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				✓	
	Infringing copyright and intellectual property (including through the use of Generative AI services)				✓	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			✓	✓	
	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				✓	

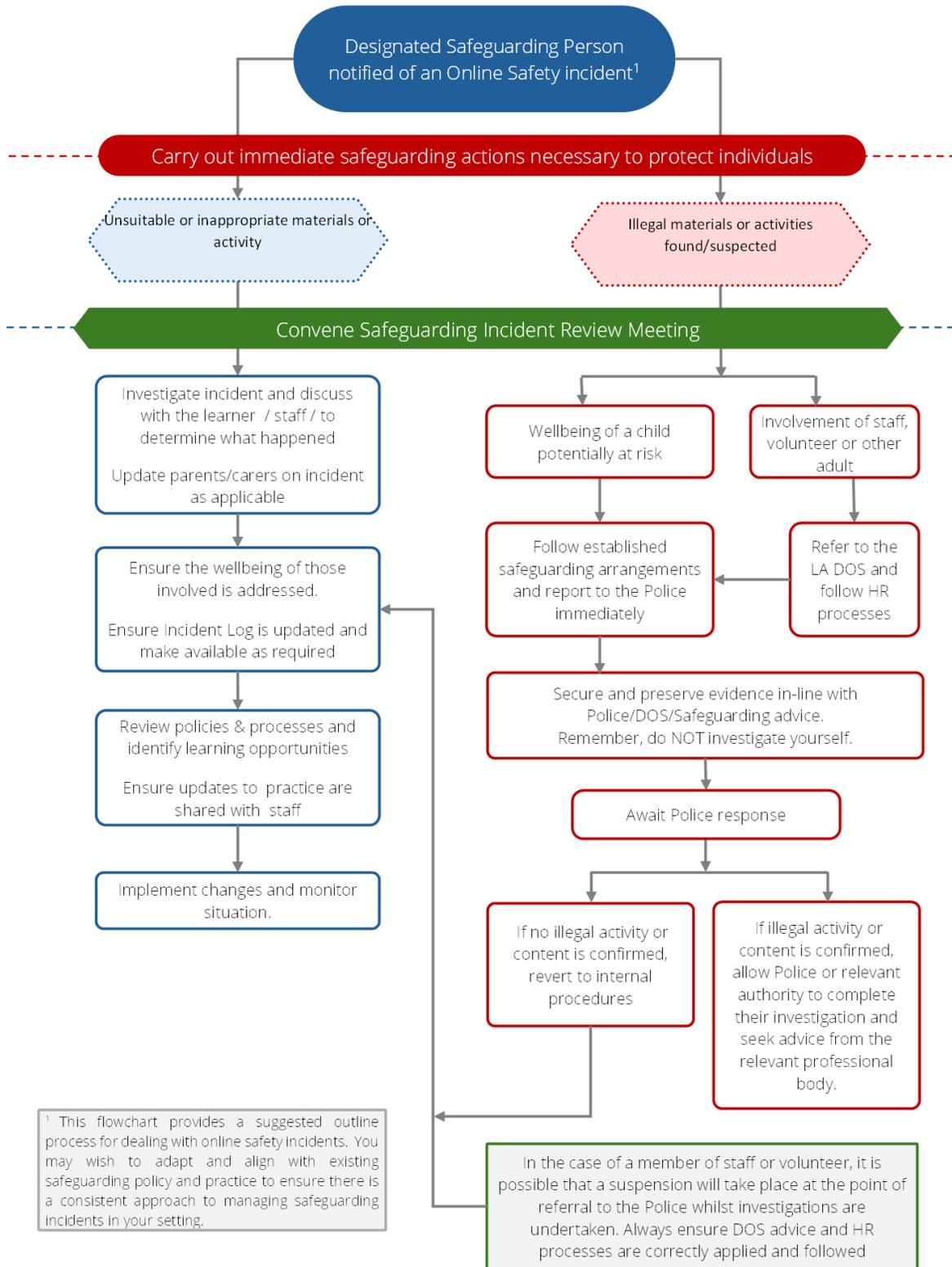
- 5.5. When using communication technologies, the school considers the following as good practice:
- when communicating in a professional capacity, staff should ensure that the communication tools they use are officially sanctioned by the school
 - any digital communication between staff and learners or parents/carers (email, social media, learning platform, etc.) must be professional in tone and content. Personal email addresses, text messaging or social media must not be used for these communications.
 - 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
 - relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school email addresses should be used to identify members of staff and learners.

6. REPORTING AND RESPONDING

- 6.1. 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.
- 6.2. 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.
- 6.3. 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
- 6.4. 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
- where Generative AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that Generative AI might miss
- as long as there is no suspected illegal activity, devices may be checked using the following procedures:
 - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
 - conduct the procedure using a designated computer that will not be used by learners and if necessary can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same computer for the duration of the procedure.
 - it is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
 - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form **(except in the case of images of child sexual abuse – see above)**.
 - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - internal response or discipline procedures
 - involvement by local authority (as relevant)
 - police involvement and/or action
 - it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
 - there are support strategies in place e.g. peer support for those who are reporting or are affected by an online safety incident
 - incidents should be logged by using the school's designated safeguarding process.



- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; [Professionals Online Safety Helpline](#); [Reporting Harmful Content](#); [CEOP](#); [Keeping safe online](#) on Hwb
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
 - the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
 - staff, through regular briefings
 - learners, through assemblies/lessons
 - parents/carers, through newsletters, school social media, website
 - governors, through regular safeguarding updates
 - local authority/external agencies, as relevant
- The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

7. SCHOOL ACTIONS

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:

Responding to Learner Actions

Incidents	Refer to class teacher/tutor	Refer to Head of AOLE/ HoF/ HoS	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).		✓	✓	✓	✓	✓	✓		✓
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		✓					✓	✓	✓
Corrupting or destroying the data of other users.		✓	✓			✓	✓		✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature * If the content is threatening, discriminatory, sexually inappropriate, or involves safeguarding concern		✓		✓*		✓	✓		✓
Unauthorised downloading or uploading of files or use of file sharing.		✓			✓	✓	✓		✓

Incidents	Refer to class teacher/tutor	Refer to Head of AOLE/ Head of AOLE/ HoF/ HoS	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
Using proxy sites or other means to subvert the school's filtering system.		✓			✓	✓	✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident.		✓				✓		✓	
Deliberately accessing or trying to access offensive or pornographic material.		✓	✓	✓	✓	✓	✓		✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.		✓			✓	✓	✓		✓
Unauthorised use of digital devices (including taking images) *If images involve illegal content (e.g., child exploitation), or if safeguarding concerns arise		✓	✓*	✓*		✓	✓		✓
Unauthorised use of online services	✓	✓				✓	✓		✓
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school. *If the actions involve illegal activity or safeguarding concerns.		✓	✓	✓*		✓	✓		✓
Continued infringements of the above, following previous warnings or sanctions.		✓	✓		✓	✓	✓		✓

Responding to Staff Actions

Incidents	Refer to line manager	Refer to safeguarding lead	Refer to Headteacher	Refer to Police	Refer to local authority technical support for advice/action	Remove device/network/internet access rights	Issue a warning	Further sanction, in with acceptable use 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).	✓	✓	✓	✓	✓	✓		✓
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	✓		✓		✓	✓		✓
Corrupting or destroying the data of other users. * If there is evidence of malicious intent or criminal damage ** If data relates to personal or sensitive learner information.	✓	✓**	✓*			✓		✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature *If the message includes threats, hate speech, or illegal content.	✓	✓	✓	✓*				✓
Unauthorised downloading or uploading of files or use of file sharing.	✓	✓	✓					✓
Using proxy sites or other means to subvert the school's filtering system.	✓	✓	✓			✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident.	✓	✓	✓		✓			✓

Incidents	Refer to line manager	Refer to safeguarding lead	Refer to Headteacher	Refer to Police	Refer to local authority technical support for advice/action	Remove device/network/internet access rights	Issue a warning	Further sanction, in with acceptable use policy
Deliberately accessing or trying to access offensive or pornographic material.	✓	✓	✓	✓	✓	✓		✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act. *Potential legal or regulatory violation.	✓		✓*		✓	✓		✓
Unauthorised use of digital devices (including taking images) *If images were stored, shared, or accessed through school systems. **If the content taken or shared is illegal or raises serious safeguarding concerns.	✓	✓	✓	✓**	✓*			✓
Unauthorised use of online services	✓		✓				✓	✓
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school. * If the action compromises learner safety, welfare, or school safeguarding standards.	✓	✓*	✓					✓
Continued infringements of the above, following previous warnings or sanctions.	✓	✓	✓	✓	✓	✓		✓

8. THE USE OF GENERATIVE ARTIFICIAL INTELLIGENCE (GENAI) SYSTEMS IN SCHOOL

- 8.1. 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.
- 8.2. 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.
- 8.3. 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.
- 8.4. The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.
- 8.5. 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.
- 8.6. We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Learners Safe
- 8.7. 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.
- 8.8. 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.
- 8.9. 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.
- 8.10. 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 comply with standards set by the Information Commissioner's Office (ICO) before using them for work related to the school.

- 8.11. 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.
- 8.12. 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.
- 8.13. 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.
- 8.14. 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.
- 8.15. Staff must report any incidents involving gen AI misuse, data breaches or inappropriate outputs immediately to the relevant internal teams.
- 8.16. The school will keep a record of all tools in use, their purpose and potential risks.
- 8.17. 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.
- 8.18. The school will support parents and carers in their understanding of the use of gen AI in the school
- 8.19. 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.
- 8.20. Staff will ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance.
- 8.21. Staff will ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing.
- 8.22. 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.

9. EDUCATION

Online Safety Education Programme

- 9.1. 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.

- 9.2. 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:
 - 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

9.3. [Keeping Learners Safe](#) states:

“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.”

- 9.4. 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
 - learners contribute to the online safety education programme e.g. digital leaders leading lessons for younger learners, online safety campaigns
 - 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

- 9.5. 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 Online Safety Lead and Designated Safeguarding Person will receive regular updates through attendance at external training events, 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

- 9.6. **Governors should take part in online safety training / awareness sessions**, with particular importance for those who are members of any sub-committee or link 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 or other relevant organisation (e.g. SWGfL)
 - participation in school training / information sessions for staff or parents.
- 9.7. 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

- 9.8. 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

- 9.9. 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.

- 9.10. 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 (for early years settings please refer to the [Online Safety Toolkit for early years practitioners](#))
- 9.11. 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.
- 9.12. The school is committed to sharing its good practice with other schools and education settings.

10. 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.

11. FILTERING

- 11.1. The school filtering policies are agreed and managed by the Local Authority and systems are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents and behaviours
- 11.2. The Local Authority 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](#)
- 11.3. Internet access is filtered for all users
- 11.4. 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.
- 11.5. 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
- 11.6. There is a clear process in place to deal with requests for filtering changes.
- 11.7. 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.)
- 11.8. Younger learners will use child friendly/age-appropriate search engines e.g. Google safe search.
- 11.9. There is an appropriate and balanced approach to providing access to online content according to role and / or need
- 11.10. 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.*

- 11.11. *Where personal mobile devices are permitted for use, there is clear separation between the school network filtering and the associated guest network filtering.*
- 11.12. *The system manages access to content through non-browser services (e.g. apps and other mobile technologies)*
- 11.13. If necessary, the school will seek advice from, and report issues to, the [Report Harmful Content](#) site.

12. MONITORING

- 12.1. 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.
- 12.2. **Users are made aware, through the acceptable use agreements, that monitoring takes place.**

13. TECHNICAL SECURITY

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 by ExtraScope who will keep an up-to-date record of users and their usernames
- 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 Key Stage 2 and above should increase as learners progress through school
- ExtraScope 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 (to be described) 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 network
- where Gen AI systems are used for technical security, their effectiveness is regularly reviewed, 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.

14. DEVICES

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

14.2. The school allows:

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	Yes	No
Full network access	Yes	Yes	Yes	No	No	No
Internet only	No	No	No	No	Yes	No
No network access	No	No	No	No	Yes	No

School-Owned / Provided Devices

The use of school-owned digital devices (e.g., laptops, tablets, Chromebooks, phones) is governed by the following provisions:

14.3. Device Allocation

Devices will be allocated by the school to staff and learners based on role-specific requirements, curriculum needs, or inclusion support. Allocation is approved by senior leaders or the IT lead and recorded centrally.

14.4. Permitted Use: Time, Location, and Context

Use of school devices is permitted during designated times and in approved areas.

- **In-school use** is allowed in classrooms, offices, and workspaces unless otherwise stated.
- **Mobile-free zones** (e.g., changing rooms, toilets, pastoral rooms) must be respected at all times.
- **Out-of-school use** (e.g., at home) requires prior approval and adherence to school monitoring protocols.

14.5. Personal Use

Limited personal use of school devices may be permitted outside of teaching hours, provided it:

- Does not interfere with work duties or network performance
- Does not violate any part of the Acceptable Use Policy
- Is compliant with safeguarding and data protection regulations

14.6. Network and Internet Access Levels

Users will be granted access appropriate to their role (e.g., staff vs learner). Access may be restricted or filtered based on content type, time of day, or location. Admin-level privileges are reserved for authorised personnel only.

14.7. Device Management and Configuration

All school devices are centrally managed. Users must not:

- Install unapproved software or apps
- Change settings that affect security or functionality
- Disable antivirus or monitoring tools

Device activity may be monitored in compliance with school policy and legal frameworks.

14.8. Network/Broadband Capacity

Device usage must not exceed acceptable network load or interfere with school-wide access. Streaming, gaming, or large file transfers may be restricted to preserve bandwidth.

14.9. Technical Support

IT support is available through the school's helpdesk or designated technical support provider. All faults, damage, or security concerns must be reported immediately.

14.10. Filtering and Monitoring

School devices are subject to web filtering and monitoring tools to prevent access to inappropriate or harmful content. Attempting to bypass filters is a policy violation.

14.11. Cloud Service Access

Devices may access approved cloud platforms (e.g., Microsoft 365, Google Workspace) for educational and administrative purposes. Use of unapproved third-party storage services is prohibited.

14.12. Use on Trips/Events

Use of school devices during off-site trips or events must be pre-approved and supervised. Devices must be handled responsibly and used only for educational purposes.

14.13. Data Protection and Privacy

All users must ensure compliance with GDPR and the school's Data Protection Policy. Personal or sensitive data must be encrypted, securely stored, and not downloaded to unencrypted devices.

14.14. Images and Recordings

Taking, storing, or sharing images/audio/video on school devices must follow the school's safeguarding, consent, and media policies. Devices must not be used to capture content in prohibited areas.

14.15. Exit/Leaver Procedures

Upon leaving the school, users must return all devices and accessories. Access to school software, cloud services, and stored data will be revoked. Any personal data must be removed before handover.

14.16. Liability for Damage

Users are responsible for the care of school devices issued to them. Wilful damage or negligence may result in repair costs or disciplinary action.

14.17. Training and Support

All staff will receive training on the safe and effective use of school devices, including safeguarding, data protection, and software use. Ongoing CPD opportunities will be provided.

Personal devices

The use of personal devices on school premises must be safe, responsible, and compliant with school policies and legal frameworks. This section sets out clear expectations for staff and visitors using personal mobile devices on school premises.

14.18. User Eligibility

Only staff and approved visitors are permitted to use personally owned devices on school premises. Learners are not permitted to use personal devices unless specific written permission has been granted (e.g., for accessibility reasons).

14.19. Use Restrictions: Time, Location, and Context

- Personal device use must be limited to staff rooms, offices, or designated areas during non-contact or break times.
- Devices must not be used in learner-facing areas (classrooms, corridors, playgrounds) unless explicitly approved for educational purposes.
- Mobile-free zones (e.g., toilets, changing areas, safeguarding-sensitive spaces) must be strictly respected.
- Phone calls or private use must never interrupt teaching, supervision, or professional duties.

14.20. Use for School Business

Staff may use personal devices for school-related tasks, including:

- Accessing email, calendars, and learning platforms
- Conducting research or lesson preparation
- Communicating via approved school apps (e.g., ClassDojo, Seesaw)

Note: Staff must follow all data protection, security, and confidentiality policies when using personal devices for school business.

14.21. Network and Internet Access

- Staff and visitors may connect to the guest Wi-Fi network, which provides filtered internet access.
- Access to internal school networks (e.g., shared drives, MIS) is not permitted from personal devices unless managed through approved secure platforms (e.g., VPN or remote access with MFA).
- Devices must never be used to attempt to access secure internal systems unless authorised.

14.22. Network/Broadband Capacity

Use of personal devices must not compromise the performance of the school's network or impact learning. Bandwidth-intensive activities (e.g., video streaming, large downloads) may be restricted.

14.23. Technical Support

The school does not provide technical support for personally owned devices. Users are responsible for the maintenance and security of their own equipment.

14.24. Internet Filtering and Monitoring

- Personal devices connected to the school's guest Wi-Fi are subject to internet filtering to block access to inappropriate content.
- Use of mobile data (3G/4G/5G) bypasses school filtering and is discouraged on school premises.
- The school may monitor network traffic from personal devices connected to its infrastructure.

14.25. Software Licensing

- Staff and learners may be entitled to install Microsoft Office applications on personal devices through the Hwb national licensing agreement.
- Any other licensed software used for school purposes must be approved by the school and comply with licensing terms.
- The school is not responsible for licensing compliance on personally owned software unless explicitly provided.

14.26. Data Protection

- No personal device should store unencrypted personal or sensitive data relating to learners or staff.
- Staff must use secure, school-approved cloud services (e.g., Hwb, Microsoft 365) when handling such data.
- Devices must be password-protected and have lock-screen timeouts enabled.

14.27. Taking, Storing and Using Images

- The use of personal devices to take photos, videos or audio recordings on school grounds is strictly controlled.
- Any media capturing learners or staff must be for approved educational use, with prior consent, and transferred immediately to school systems for secure storage.
- Media must never be stored long-term on personal devices or shared via unapproved platforms.

14.28. Liability and Disclaimer

- The school accepts no responsibility for the loss, theft, damage, or malfunction of any personal device used on the premises or while connected to the network.
- Users connect their devices at their own risk.

14.29. Device Identification

- All personal devices used for school purposes should be clearly labelled with the user's name.
- Devices must be easily identifiable to ensure accountability and avoid misuse.

14.30. Visitor Information

- Visitors will be made aware of personal device expectations through:
 - Visitor welcome packs
 - Displayed signs in key areas
 - Verbal reminders from reception or hosting staff
- Guest Wi-Fi login details may be provided upon approval.

14.31. Education and Awareness

- Staff and learners receive regular education and training on the safe and responsible use of digital devices as part of the school's online safety curriculum.
- Topics include mobile safety, privacy, legal use, and protecting digital reputation.

14.32. Misuse and Sanctions

- **Any misuse of personal devices (e.g., accessing prohibited content, bypassing filters, unapproved recording) will result in action according to the school's disciplinary procedures.**
- Consequences may include:
 - Removal of Wi-Fi access
 - Formal warnings
 - Referral to senior leadership
 - In serious cases, safeguarding or legal referrals

15. SOCIAL MEDIA

- 15.1. 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
- 15.2. 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
- 15.3. 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.
- 15.4. 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

- 15.5. 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.
- 15.6. School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Group 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](#).
- 15.7. See the school's Social Media Policy for further information.

16. DIGITAL AND VIDEO IMAGES

- 16.1. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm (select/delete as appropriate):
- 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
- 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 and parents/carers.

17. ONLINE SAFETY MESSAGING

- 17.1. The school communicates with parents/carers and the wider community and promotes the school through:
- Public-facing website
 - Social media
 - Online newsletters
- 17.2. The school website is managed by the Assistant Headteacher (Progress and Digital Transformation). 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.
- 17.3. Where learner work, images or videos are published, their identities are protected and full names are not published.
- 17.4. 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.
- 17.5. The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process

18. DATA SECURITY

18.1. Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

18.2. The school:

- 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 Lead (DPL) 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
- 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
- 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

- has a Freedom of Information Publication Scheme 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

18.3. 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.

19. CYBER SECURITY

- 19.1. [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.”

- 19.2. The school has:

- has adopted and made use of the relevant Hwb [Network and Data Security Standards](#)
- in partnership with their education technology support partner, identified the most critical parts of the school’s digital and technology services and sought assurance about their cyber security
- in partnership with their education technology support partner, an effective backup and restoration plan in place in the event of cyber attacks
- governance and IT policies that reflect the importance of good cyber security
- provided staff 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.

20. 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.

APPENDIX A: LEARNER ACCEPTABLE USE AGREEMENT - LOWER SCHOOL PUPILS

Our Technology Rules

I will follow these rules to use computers, tablets and the internet safely 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, games or websites my teacher says are safe.

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.
- I will ask for help from a trusted adult if I am not sure what to do or if I think I may have done something wrong.

What Happens If I Forget the Rules

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

APPENDIX B: LEARNER ACCEPTABLE USE AGREEMENT - MIDDLE AND UPPER SCHOOL PUPILS

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

Learner Acceptable Use Agreement Form

I agree to use the school's digital systems 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, 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 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 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 fact-check and critically evaluate AI-generated content for accuracy, bias, and discrimination before sharing or publishing.
- 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 cybersecurity poses a risk to both me, other learners and the school and will ensure I take precautions before accessing emails, messages or links. I will check with trusted adults if I have any such concerns.
- I will immediately report any damage, faults or failings involving equipment or software, however this may have happened.
- I will follow the age requirements for social media, apps, and tools.
- 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 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 will ensure my behaviour reflects positively on the school, both in and out of school settings.

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.

APPENDIX C: ACCEPTABLE USE AGREEMENT - STAFF AND VISITORS

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 using the internet and 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 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 the school will monitor my use of school devices and digital technology systems
- 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 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 illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using digital technologies and systems: (schools should amend this section in the light of relevant policies):

- 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 and parents/carers using official school 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.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will abide by all relevant guidance and legislation (e.g. Keeping Learners Safe / 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
- When using Generative Artificial Intelligence (Gen AI) systems in my professional role I will use these responsibly and:
 - will only use Gen AI tools approved by the school
 - will be aware of the risks of bias and discrimination, critically evaluating the outputs of Gen 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 Gen 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
 - when I use my personal mobile devices in school, I will follow the rules set out by the school, , in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus / anti-malware software and are free from viruses.
 - 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 ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not access illegal, inappropriate or harmful content on school systems.
- I will not bypass any filtering or security systems that are used to prevent access to such content.
- 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 immediately report any damage or faults involving equipment or software; however this may have happened.

When using the internet 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 Generative AI has been used.
- 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 this acceptable use agreement applies to my use of digital technologies related to my professional responsibilities, within or outside of the school
- I will ensure my use of technologies and platforms is in line with the school's agreed codes of conduct
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include 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.