

Online Safety Policy



Annotation Key for this Document

PNM Mr Phil Meredith, Associate Assistant Headteacher

ASG Mr Anthony Gardner, Assistant Headteacher

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

Development/monitoring/review of this policy

Schedule for development/monitoring/review

This online safety policy was approved by the governing body/governors sub-committee on:	
The implementation of this online safety policy will be monitored by the:	SLT lead – Mr A Gardner
The governing body/governors sub-committee will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	June each year
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	June 2026
Should serious online safety incidents take place, the following external persons/agencies should be informed:	LA Safeguarding officers – Police



Roles and responsibilities

The following section outlines the online safety roles and responsibilities of individuals¹ and groups within the school .

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing Body receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body should take on the role of online safety governor to include:

- regular meetings with the online safety coordinator/officer
- regular monitoring of online safety incident logs
- regular monitoring of filtering change control logs and monitoring of filtering logs (where possible)
- reporting to relevant governors/sub-committee/meeting.

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety may be delegated to the online safety coordinator/officer.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- The headteacher/senior leaders are responsible for ensuring that the online safety coordinator/officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles

Technical staff and SLT

The school's technical staff and SLT in conjunction with our IT partner will:

- the schools' 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 or other relevant body and also the online safety policy/guidance that may apply
- 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 network/internet/learning platform(Google |Classroom)/Hwb/remote access/e-mail is regularly monitored in order that any misuse/attempted misuse can be reported to the SLT lead on online safety; for investigation/action/sanction
- monitoring software/systems are implemented and updated as agreed in school policies

Teaching and support staff

These individuals are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school online safety policy and practices. Delivered through professional learning and remote learning activities.
- they have read, understood and signed the staff acceptable use agreement (AUA)
- they report any suspected misuse or problem to the relevant member of SLT and/or technical staff
- all digital communications with learners/parents and carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities

- learners understand and follow the online safety and acceptable use agreements
- learners have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, 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 checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated senior person

The designated senior person, and safeguarding officers 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.
- Misuse and dangers of Ai

Learners

These individuals:

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement (including personal devices – where allowed)
- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- understand the implications of using Generative Ai to plagiarise work
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online bullying
- understand the implications of using Generative Ai to produce harmful fake images and other media
- 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

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents and carers understand these issues through parent forums, newsletters, letters, website, Hwb development information, the Hwb learning platform and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents'/carers' sections of the website
- their children's personal devices in the school.

Community users

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

Policy statements

Education – learners

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 a range of subjects, topic areas should be regularly revisited.

- Key online safety messages should be reinforced as part of a planned programme of assemblies, TFTH (Thoughts for the day) and tutorial/pastoral activities
- 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
- Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- 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 monitoring the content of the websites the young people visit. Further supported by the schools filtering systems and Impero software
- Learners should also be made aware of the potential **harmful uses of AI** and be guided in how to engage with these technologies safely and ethically. This includes understanding that AI-generated content can sometimes be biased, inaccurate, or misleading, and that not all outputs from tools like ChatGPT or image generators are reliable or appropriate. Students should be taught not to input personal or sensitive information into AI tools and to be cautious of AI that mimics real people or spreads disinformation. Discussions around deepfakes, AI-assisted cheating, and online manipulation should form part of the school's digital literacy programme. Learners must be encouraged to think critically, verify information from multiple sources, and report any concerning or inappropriate AI-related content to a trusted adult or staff member.
- It is accepted that from time to time, for good educational reasons, students 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 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.

Education – parents and carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- letters, newsletters, web site, learning platform, Hwb
- parent forums
- high profile events/campaigns, e.g. Safer Internet Day

Education and training – staff/volunteers

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

A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.

- all new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- ASG and/or PNM 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, and PLB opportunities.
- the online safety coordinator/officer (or other nominated person – ASG/PNM) will provide advice/guidance/training to individuals as required.

Training – governors

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

- attendance at training provided by the local authority/National Governors Association/or other relevant organisation, (e.g. SWGfL)
- participation in school training/information sessions for staff or parents

Technical – infrastructure/equipment, filtering and monitoring

The school has a managed ICT service provided by IT partner. It is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school. The managed service provider is fully aware of the school online safety policy/acceptable use agreements. The school also checks the local authority/ policies on these technical issues if the service is not provided by the authority.

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

There will be regular reviews and audits of the safety and security of school technical systems.

- Servers, wireless systems and cabling must be securely located and physical access restricted.
- Good practice in preventing loss of data from ransomware attacks requires a rigorous and verified back-up routine.
- All school networks and system will be protected by secure passwords.
- The master account passwords for the school systems should be kept in a secure place, e.g. school safe. Consideration should also be given to using two factor authentication for such accounts.
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Technical staff and will be reviewed, at least annually, by the online safety group
- All users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords must not be shared with anyone.
- All users will be provided with a username and password by the Technical staff who will keep an up to date record of users and their usernames.

- Good practice highlights that passwords over 12 characters in length are more difficult to crack. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.
- Technical staff are 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.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- There is a clear process in place to deal with requests for filtering changes.
- The school provides enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users: staff/learners, etc.).
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Where possible, school technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- 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.
- 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 policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place on the appropriate use of Ai for all staff and learners.

Mobile technologies

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

- The school acceptable use agreements for staff, learners, parents and carers will give consideration to the use of mobile technologies.
- The school allows:

	School devices		Personal devices	
	School owned for individual use	School owned for multiple users	Student owned	Staff owned
Allowed in school	Yes	Yes	No – Mobile devices are not permitted to be used. Gate to gate policy in place. Exception for 6 th formers in common	Yes

			room and study areas	
Full network access	Yes	Yes	Student BYOD	Yes - Staff BYOD

Aspects that the school may wish to consider and include in their online safety policy, mobile technologies policy or acceptable use agreements include the following:

School owned/provided devices

School devices for students will be either in the form of Desktop computers for dedicated ICT suites, or Chromebooks/tablets. These will be restricted to school use unless there are extenuating circumstances. These are for educational use only and will be managed through school filtering systems and protocols in line with recommended guidance. Work will be backed up on in house servers alongside where appropriate cloud based storage through either the Google or Hwb infrastructure. Technical support for these devices will be provided by technical staff alongside additional support provided by IT partner. All information obtained will be compliant with the Data Protections Act 2018.

Data will be stored for an appropriate amount of time in line with the 2018 data protection act. It will be the school's responsibility to remove users from the school ICT infrastructure once they are classified as school leavers. Accidental damage of any ICT equipment will be covered by the school and school warranties. Malicious damage will be the responsibility of the student/parent/carer to cover in line with the acceptable usage agreements.

Personal devices

Staff/visitors and KS5 learners are allowed to bring personal ICT devices to school. In order to link to the school infrastructure, the user must adhere to and sign an acceptable usage agreement. Personal devices are the responsibility of the user and the school will not accept liability for any damage/loss or malfunction of equipment. If connected to the network the devices will be subject to the same filtering protocols as other devices. No technical support will be available for personal devices. The use of personal ICT equipment is permitted; however, this must adhere to data protection protocols. The use of personal ICT equipment is permitted; however, this must adhere to safeguarding and data protection protocols. Personal devices may be used by staff to capture images or video for legitimate educational purposes (e.g. lessons, trips, performances or enrichment activities), provided this is in line with the Safeguarding Policy, parental consent arrangements, and this Online Safety Policy.

Any images or video must be transferred to a secure school system as soon as possible and deleted from the personal device. Personal devices must not be used for the long-term storage or sharing of pupil images and must not be used in sensitive areas (e.g. changing rooms).

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and carers and learners need to be aware of the risks associated with publishing digital images on the internet. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm

- 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.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the capture, storage, sharing and publication of those images. Images should preferably be taken on school equipment; however, staff may use personal devices where

necessary, provided this is authorised, for school purposes only, and images are transferred securely to school systems and deleted from the personal device at the earliest opportunity.

- 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 published on the school website
- Learners' work can only be published with the permission of the learner and parents or carers.

Data protection

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

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

- data must be encrypted and password protected.
- device must be password protected.
- device must be protected by up to date virus and malware checking software
- data must 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
- will not transfer any school personal data to personal devices except as in line with school policy
- 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 and secure password protected devices.
- data storage on removable media is not permitted.

Communication

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

- the official school e-mail service may be regarded as safe and secure and is monitored. Users should be aware that e-mail communications are monitored.
- All comms should be in line with the school's communication code (available on the school website)
- users must immediately report to the 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
- any digital communication between staff and learners or parents/carers (e-mail, chat, learning platform, etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal e-mail addresses, text messaging or social media must not be used for these communications
- learners should be taught that email and communication to staff should be polite and formal in tone
- learners should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- personal information should not be posted on the school website and only official e-mail addresses should be used to identify members of staff.

Social media

Expectations for teachers' professional conduct are set out by the Education Workplace Council but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

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
- training being provided including acceptable use, social media risks, checking of settings, data protection and reporting issues
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk.

School staff should ensure that:

- no reference should be made in social media to learners, parents and carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be 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.

When official school social media accounts are established there should be:

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

Personal use

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

Monitoring of public social media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process that defaults to the local authority for guidance on a case by case basis.

School use of social media for professional purposes will be checked regularly by a senior leader and online safety group to ensure compliance with the social media, data protection, communications, digital image and video policies.

Responding to incidents of misuse

Illegal incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the DSP Safeguarding. All safeguarding issues are to be recorded in Edukey.

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 and in line with the School's Conduct Policy.

Inappropriate Use of AI

The following behaviours are considered inappropriate and will be addressed in line with this Behaviour Policy and Welsh Government guidance:

- Using AI to create, share or promote content that causes harm, distress, embarrassment or concern to any learner or adult
- Using AI to generate abusive, discriminatory, threatening or harassing material
- Using AI to impersonate others, fabricate evidence, or manipulate images, audio or video in a way that could mislead or harm
- Using AI to support cheating, plagiarism or academic dishonesty
- Using AI to bypass school systems, monitoring or safeguarding controls
- Any use of AI that undermines the safety, wellbeing or dignity of others

Sanctions

Where inappropriate use of AI occurs, the school will apply sanctions that are:

- proportionate
- appropriate to the behaviour
- consistent with this policy
- aligned with Welsh Government guidance on behaviour, relationships and wellbeing

Sanctions may include:

- loss of digital privileges
- restorative approaches
- parental/carer meetings
- internal sanctions in line with school procedures
- **fixed-term exclusions**, where the behaviour constitutes a serious breach of the school's behaviour policy
- **permanent exclusion**, only in the most serious cases and always in line with Welsh Government statutory guidance, where the behaviour represents a serious breach of the behaviour policy and where allowing the learner to remain in school would seriously harm the education or welfare of others

Appendix

A1 Learner Acceptable Use Agreement

School policy

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. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safer internet access at all times.

This Acceptable use agreement is intended to ensure:

- that learners will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that learners will have good access to digital technologies to enhance their learning and will, in return, expect the learners to agree to be responsible users.

Acceptable use agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of systems, devices and digital communications
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it
- I will be aware of "stranger danger", when I am communicating online
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details, etc.)
- If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will only use them for personal or recreational use if I have permission
- I will only make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work, if I have permission
- I will only use the school systems or devices for online educational gaming, file sharing, or video broadcasting (eg YouTube), if I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will only access, copy, remove or alter any other user's files, with the owner's knowledge and permission
- 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 only take or distribute images of others with their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal device(s) in school if I have permission. I understand that, if I do use my own device(s) in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- **I will immediately report any damage or faults involving equipment or software, however this may have happened**
- I will only open hyperlinks in emails or attachments to emails, if I know and trust the person/organisation who sent the email, and have no concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will only install/ store programmes on a school device, if I have permission

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- where work is protected by copyright, I will not try to download copies (including music and videos)
- when I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- When using generative Ai platforms such as ChatGPT, I will only use these for research and development of my work and not to create work for me to pass off as my own

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

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online bullying, use of images or personal information)
- I understand that if I fail to comply with this acceptable use agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police. If it is work that counts towards my examinations, I may face disciplinary actions from the exam board and loss of qualifications.

Please complete the sections below / on the next page to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Learner acceptable use agreement form

This form relates to the learner acceptable use agreement; to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

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

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed), e.g. mobile phones, gaming devices, cameras etc
- I use my own equipment 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, learning platform, website, etc.

Name of Learner:

Teaching & Learning/Curriculum
Subcommittee April 2026

Group/Class

Signed:

Date:

A2 Staff (and volunteer) acceptable use agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital communications 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. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safer internet access at all times.

This acceptable use agreement is intended to ensure:

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

The school will try to ensure that staff and volunteers will have good access to digital technologies to enhance learning opportunities and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable use agreement

I understand that I must use school digital technologies in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technologies. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- 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 understand that I should not write down or store a password where it is possible that someone may steal it.
- 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 school ICT systems:

- I will only access, copy, remove or alter any other user's files, with 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 appropriate consent and in accordance with the school's policy on the use of digital/video images. I may use my personal device to record images or video for legitimate educational purposes only where this is permitted by school policy. In such cases, I will ensure that all content is transferred promptly to a secure school system and deleted from my personal device and will not be stored or shared via personal accounts or platforms.
- 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 and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school digital technology systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, extremist material or adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will only make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work, with permission
- I will only install or attempt to install/store programmes on devices or if 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 /LA Personal data policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based protected and restricted data must be held in lockable storage
- I understand that 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 permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

When using Generative Ai in my professional capacity or for school sanctioned personal use:

- I will use AI tools (e.g. ChatGPT, Microsoft Copilot) only for professional purposes, such as planning lessons, generating ideas, or creating resources — not for marking or grading unless explicitly permitted.

- I will not input personal, sensitive, or confidential information about pupils, staff, or the school into AI platforms.
- I will always fact-check AI-generated content. AI may produce inaccurate, biased, or misleading information.
- I will always clearly label and acknowledge any AI-generated content shared with students or parents to maintain transparency.
- I will not use AI to generate teaching content that violates copyright or reuses licensed material without permission.
- I will treat AI tools as assistants, not authorities – they support, not replace, professional expertise and judgement.

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

- I understand that this acceptable use agreement applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- 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 school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name:

Signed:

Date:

A3 Acceptable Use Agreement for community users

This acceptable use agreement is intended to ensure:

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

Acceptable use agreement

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

- I understand that my use of school systems and devices and digital communications will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.

- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems/devices.

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

Name Signed Date:

B1 Summary of Legislation

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

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

Legal Framework Supporting Online and Digital Conduct in Schools (Updated 2025)

Computer Misuse Act 1990

This Act makes it a criminal offence to:

- Erase or amend data or programs without permission.
- Gain unauthorised access to computer systems or data.
- Intercept communications without lawful authority ("eavesdropping").
- Misuse computer time or resources.
- Maliciously corrupt or delete digital data or software.
- Deny access to authorised users.

It underpins expectations for responsible ICT use in schools and informs Acceptable Use Agreements.

Data Protection Act 2018 (UK GDPR)

This Act controls how personal information is handled by organisations and is the UK's implementation of the General Data Protection Regulation (GDPR). It applies to all personal data processed by schools. Key principles require data to be:

- Used lawfully, fairly, and transparently.
- Collected for specified, explicit purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and kept up to date.
- Retained only as long as necessary.
- Processed securely.

Stronger legal protections apply to sensitive personal data such as health, ethnicity, biometric data (if used for identification), and religious beliefs.

Individuals have rights under the Act, including the right to access personal data, request correction or deletion, object to processing, and challenge decisions made through automated profiling.

Freedom of Information Act 2000

This legislation gives members of the public the right to access recorded information held by public authorities, including schools. Schools must respond to requests within set timeframes unless exemptions apply. Information disclosed must comply with data protection requirements.

Online Safety Act 2023

This Act introduces a new legal framework to regulate harmful online content and platform responsibility. It includes:

- Criminal offences for sending grossly offensive, obscene, indecent or menacing messages online.
- Offences for cyberflashing, sharing intimate images without consent, and encouraging self-harm.
- A statutory duty of care for online service providers to protect users, particularly children.

Schools should align safeguarding practices with the Act, especially in digital literacy and PSHE provision.

Malicious Communications Act 1988

This makes it an offence to send electronic messages (emails, texts, social media) or letters that are indecent, grossly offensive, threatening, or knowingly false, intending to cause distress or anxiety.

Regulation of Investigatory Powers Act 2000 (RIPA) and Investigatory Powers Act 2016

RIPA criminalises the unauthorised interception of communications. However, with consent from the system controller, schools may monitor communications:

- To ensure regulatory compliance.
- To demonstrate performance standards.
- To prevent or detect misuse or crime.

- To verify the business or personal nature of communications.

The 2016 Act expands surveillance powers held by public bodies and should be noted in data governance and safeguarding policies.

Trade Marks Act 1994

This protects registered trademarks from unauthorised use. It is relevant to schools when creating digital content, presentations, or student materials to ensure intellectual property is respected.

Copyright, Designs and Patents Act 1988

This Act protects literary, artistic, and media works. In a school setting, it is an offence to reproduce copyrighted material without permission, except in limited situations such as:

- Non-commercial research and private study.
- Educational use under fair dealing exemptions.
- Use of copyright-licensed resources.

It also enshrines Moral Rights, including the right of authors to be credited and not have their work misrepresented.

Criminal Justice and Public Order Act 1994 / Public Order Act 1986

These Acts criminalise the use of threatening, abusive or insulting language or behaviour intended to cause harassment, alarm, or distress. This extends to digital communication and supports anti-bullying procedures.

Racial and Religious Hatred Act 2006 / Public Order Act 1986

These laws prohibit inciting hatred based on race or religion, including publishing or distributing threatening material. They are relevant to preventing discriminatory behaviour or hate speech within school communities.

Protection from Harassment Act 1997

It is a criminal offence to pursue a course of conduct that causes harassment, alarm, or distress. This includes online harassment, cyberstalking, and repeated unwanted contact.

Protection of Children Act 1978

This Act makes it illegal to take, make, possess, distribute, or advertise indecent images of children (under 18), including digitally manipulated or pseudo-images. It carries severe penalties and underpins safeguarding responsibilities.

Sexual Offences Act 2003

This legislation defines grooming offences, including communicating with a child under 16 online with intent to meet and commit a sexual offence. It also prohibits causing children to view sexual acts and prohibits sexual activity by individuals in a position of trust with persons under 18.

Obscene Publications Acts 1959 and 1964

It is a criminal offence to publish or electronically transmit material deemed obscene and likely to deprave or corrupt its audience. This is relevant to filtering and reporting procedures for school networks.

Human Rights Act 1998

This Act embeds rights from the European Convention on Human Rights into UK law. In the school context, relevant rights include:

- The right to privacy.
- The right to education.
- Freedom of expression (balanced with safeguarding).
- Protection from discrimination and degrading treatment.

These rights must be balanced with the safeguarding duties placed upon schools.

Protection of Freedoms Act 2012

This Act requires that schools obtain written parental consent to use biometric data (e.g., fingerprint recognition systems). Schools must explain how data will be used, stored, and protected.

Counter-Terrorism and Security Act 2015

This Act underpins the Prevent duty, requiring schools to safeguard pupils from being drawn into extremism. It includes promoting resilience, challenging extremist narratives, and working with external agencies when concerns arise.

Use of AI by Staff

When used for planning or resource creation, AI tools should be used critically and must not substitute professional judgement or breach copyright.

Digital Wellbeing

The school recognises the importance of supporting students' digital wellbeing. Learners will be encouraged to maintain healthy screen time habits, take regular breaks, and reflect on the emotional impact of social media, gaming, and online communication.

Cyber Security and Ransomware

The school will actively monitor cyber threats, including phishing, credential theft, and ransomware. Staff will receive regular training to identify and report suspicious activity. A secure backup system is in place to ensure continuity of learning in the event of cyber disruption.

Compliance with Statutory Guidance

This policy aligns with relevant statutory guidance, including *Keeping Learners Safe*, *Keeping Children Safe in Education (Wales)*, and the *Digital Competence Framework*.

Online Hoaxes, Misinformation and Reputational Harm

Staff and learners will be trained to recognise and respond appropriately to online scams, misinformation, viral challenges, and reputation-damaging content. These concerns will be handled through the safeguarding and digital safety protocols.

Misuse of School Branding or Identity

The unauthorised use of the school's logo, branding, or identity—including impersonation on social media or AI platforms—is strictly prohibited and may result in disciplinary or legal action.

Policies Equality Statement

At Caerleon Comprehensive School, we serve a diverse community and take account of a wide range of needs. In accordance with the Equality Act (2010), our policies and learning and teaching strategies fulfill our duty to serve people according to their needs and promote equality. In order to embed fairness in all aspects of school life, we take account of equality as we formulate, develop and update school policies and plans.

Our vision and values promote inclusivity and equality and tackle discrimination. We have high expectations for all our pupils and staff. Our equality statement is guided by core principles:

- All learners are of equal value;
- We recognise and respect difference;
- We foster positive attitudes and relationships and a shared sense of community and belonging;
- We observe good practice in recruitment, retention and staff development;
- We aim to reduce and challenge barriers to equality at every opportunity