Greenmeadow Primary School

Ysgol Gynradd Maesglas

‘Empowering Young Minds for Tomorrow’

Title	**Online Safety Policy**
Date	**October 2025**
Review	**October 2026**
Author	**Headteacher/SLT**

Purpose:

This Online Safety Policy outlines the commitment of Greenmeadow Primary School to safeguard members of our school community online in accordance with principles of open government and with the law. Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced as outlined in the attached 'Legislation' Appendix.

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

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

Policy development, monitoring and review

This Online Safety Policy has been developed by the Senior Leadership Team:

- *headteacher/senior leaders*
- *digital leader*
- *staff – including teachers/education practitioners/support staff/technical staff*
- *governors*
- *parents and carers*
- *community users*

Schedule for development, monitoring and review

This Online Safety Policy was approved by the *school governing body on:*	*October 2024*
The implementation of this Online Safety Policy will be monitored by:	*Headteacher*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*Annually*

Roles and responsibilities:

The following section outlines the online safety roles and responsibilities of individuals 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 and the online safety group
including the designated online safety governor receiving regular information about online safety incidents and monitoring reports.
regular meetings with the online safety coordinators
• 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 coordinators
• 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**3**
• The headteacher/senior leaders are responsible for ensuring that the online safety coordinators 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
• The headteacher/senior leaders will receive regular monitoring reports from the online safety coordinators

Online safety coordinators
Overall responsibility of online safety lies with the senior management team and safeguarding team.
However, the online safety coordinators play a significant role in ensuring the day to day monitoring and
management of online safety.
The online safety coordinators work with senior management to:
• Lead the online safety group
• take day to day responsibility for online safety issues and has a leading role in establishing and
reviewing the school online safety policies/documents alongside the senior management and safe
guarding team
• ensures that all staff are aware of the procedures that need to be followed in the event of an online
safety incident taking place.
• provides (or identifies sources of) training and advice for staff
liaises with the local authority/relevant body
• liaises with (Local authority and SRS) technical staff
• receives reports of online safety incidents and creates a log of incidents to inform future online
safety developments
• meets regularly with online safety governor to discuss current issues, review incident logs and if
possible, filtering change control logs
• liaises with senior management who attend relevant meeting/sub-committee of governors
• reports regularly to headteacher/senior leadership team/safeguarding officers.

Network manager/technical staff
The local authority/managed service provider is responsible for ensuring that:
• 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 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, in which passwords are regularly changed
• 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/Hwb/remote access/e-mail is regularly monitored
in order that any misuse/attempted misuse can be reported to the headteacher/senior leader; online
safety coordinators for investigation/action/sanction
• (if present) monitoring software/systems are implemented and updated as agreed in school policies
• the local authority filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person

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
• they have read, understood and signed the staff acceptable use agreement (AUA)
• they report any suspected misuse or problem to the headteacher/senior leader; online safety coordinators, safe guarding officers) for investigation/action
• 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, 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 checked as suitable
for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Learners
These individuals:
• are responsible for using the school digital technology systems in accordance with the learner
acceptable use agreement (this should include personal devices – where allowed)
• should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
• 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

• 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 parents'/carers' evenings, newsletters, letters, website,
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, Hwb, learning platform and online learner Records
• be kept up to date via letters, newsletters, website, learning platforms and Hwb.
• their children's personal devices in the school (where this is allowed).
• parents should be encouraged to report online bullying via social media platforms directly to the police or online via Gwent Police.

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

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 online safety provision. Learners need the help and support of the school
to recognise and avoid online safety risks and build their resilience.
Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety
messages across the curriculum. The online safety curriculum should be broad, relevant and provide
progression, with opportunities for creative activities and will be provided in the following ways (Note:

statements will need to be adapted, depending on school structure and the age of the learners).
• A planned online safety curriculum across a range of subjects, (e.g. ICT/PSE/DCF) 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.
• 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.
• 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 (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.

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
• parents and carers evenings/sessions

high profile events/campaigns, e.g. Safer Internet Day
• reference to the relevant websites/publications, e.g. hwb.wales.gov.uk/ www.saferinternet.org.uk/ www.childnet.com/parents-and-carers

Education – the wider community
The school will provide opportunities for local community groups/members of the 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, digital literacy and online
safety
• online safety messages targeted towards grandparents and other relatives as well as parents.
• the school learning platform, Hwb, website will provide online safety information for the wider
community
• supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary
groups to enhance their online safety provision

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. It is expected that some staff will identify online safety as a training need within the performance management process
• 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.
• the online safety coordinators will receive regular updates through attendance at external training events, (e.g. from Consortium/SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations
• this online safety policy and its updates will be presented to and discussed by staff in staff/team
meetings/INSET days
• the online safety coordinators (or other nominated person) 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

Mobile technologies
Mobile technology devices may be school owned/provided or personally owned and might include
smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the
school's/college's wireless network. The device then has access to the wider internet which may include
the school learning platform and other cloud-based services such as e-mail and data storage.
All users should understand that the primary purpose of the use of mobile/personal devices in a school
context is educational. The mobile technologies policy should be consistent with and inter-related to
other relevant school polices including but not limited to those for safeguarding, behaviour, anti-bullying,
acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education
programme.

Data protection
Personal data will be recorded, processed, transferred and made available according to the current
data protection legislation.
The school must ensure that:
• it has a Data Protection Policy.
• it implements the data protection principles and is able to demonstrate that it does so.
• it has paid the appropriate fee Information Commissioner's Office (ICO)
• it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest. The school may also
wish to appoint a Data Manager and Systems Controllers to support the DPO
• it has an 'information asset register' in place and knows exactly what personal data it holds, where,
why and which member of staff has responsibility for managing it
• the information asset register 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
• it will hold the minimum personal data necessary to enable it to perform its function and it will not
hold it for longer than necessary for the purposes it was collected for. The school should develop
and implement a 'retention schedule" to support this
• data held must be accurate and up to date where this is necessary for the purpose you hold it for.

Have systems in place to identify inaccuracies, such as asking parents to check emergency contact
details at suitable intervals
• it provides staff, parents, volunteers, teenagers and older children with information about how the
school / college looks after their data and what their rights are in a clear Privacy Notice
• procedures must be in place to deal with the individual rights of the data subject, e.g. one of the
dozen rights applicable is that of Subject Access which enables an individual to see to have a copy
of the personal data held about them
• data Protection Impact Assessments (DPIA) are carried out where necessary. For example, 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
• it has undertaken appropriate due diligence and has GDPR compliant contracts in place with any
data processors
• it understands how to share data lawfully and safely with other relevant data controllers. In Wales,
schools and colleges should consider using the Wales Accord on Sharing Personal Information
toolkit to support regular data sharing between data controllers
• there are clear and understood policies and routines for the deletion and disposal of data
• it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware
of the breach as required by law. It also reports relevant breaches to the individuals affected
as required by law. In order to do this it has a policy for reporting, logging, managing, investigating
and learning from information risk incidents.
• If a maintained school, it must have a Freedom of Information Policy which sets out how it will deal
with FOI requests.
• all staff receive data protection training at induction and appropriate refresher training thereafter.
Staff undertaking particular 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.
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
• can help data subjects understands their rights and know how to handle a request whether verbal
or written. 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 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.

Social media
With an increase in use of all types of social media for professional and personal purposes a policy that
sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages
should include the protection of learners, the school and the individual when publishing any material
online.
Expectations for teachers' professional conduct are set out by the General Teaching Council Wales
(GTCW) 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.
All schools and local authorities have a duty of care to provide a safe learning environment for learners
and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees
in the course of their employment. Staff members who harass, bully online, discriminate on the grounds
of sex, race or disability or who defame a third party may render the school or local authority liable to
the injured party. Reasonable steps to prevent predictable harm must be in place. All staff working at
any educational establishment are expected to demonstrate a professional approach and respect for
learners and their families and for colleagues and the learning setting.

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 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 proactively 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.
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.

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. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. 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.

• 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, distribution and publication of those images.

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 published on the school website (see parents and carers acceptable use agreement in the Appendix).

• Learners' work can only be published with the permission of the learner and parents or carers.

Appendix

Learner actions

Incidents	Refer to class teacher/tutor	Refer to Head of Department/ Head of Year/ other	Refer to Headteacher/Principal	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Issue a warning	Further sanction, e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X		X			
Unauthorised use of non-educational sites during lessons.	X					X			
Unauthorised use of mobile phone/digital camera/other mobile device.	X					X			
Unauthorised use of social media/messaging apps/personal e-mail.	X					X			
Unauthorised downloading or uploading of files.	X					X			
Allowing others to access school network by sharing username and passwords.	X					X			
Attempting to access or accessing the school network, using another learners' account.	X					X			
Attempting to access or accessing the school network, using the account of a member of staff.	X					X			
Corrupting or destroying the data of other users.	X					X			

Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.	X	X		X		X			
Continued infringements of the above, following previous warnings or sanctions.	X	X		X		X			
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X	X	X		X			
Using proxy sites or other means to subvert the school's filtering system.	X		X	X		X			
Accidentally accessing offensive or pornographic material and failing to report the incident.	X		X		X	X			
Deliberately accessing or trying to access offensive or pornographic material.	X		X	X	X				
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	X		X		X	X			

Staff Actions

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

Inappropriate personal use of the internet/social media/personal e-mail	X	X	X	X				
Unauthorised downloading or uploading of files.	X	X	X	X				
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	X	X	X	X				
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X	X						
Deliberate actions to breach data protection or network security rules.	X	X	X	X				
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X				
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.	X	X	X	X		X		
Using personal e-mail/social networking/messaging to carrying out digital communications with learners and parents/carers	X	X	X			X		
Actions which could compromise the staff member's professional standing	X	X	X	X				
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X	X	X				
Using proxy sites or other means to subvert the school's filtering system.	X	X	X	X				

Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X	X	X		X	X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X		X	X	
Breaching copyright or licensing regulations.	X	X	X	X				
Continued infringements of the above, following previous warnings or sanctions.	X	X	X		X