Rogerstone Primary School

Online Safety Policy

MAETHU
YSBRYDOLI
CYFLAWNI

Rogerstone Primary School

NURTURE
INSPIRE
ACHIEVE

Our vision

Nurture, Inspire, Achieve

To achieve our vision statement we will ensure a safe, secure, happy learning environment, that provides a variety of opportunities for all, making learning fun, that will allow every child to develop life long skills for the future and to reach their full potential.

Our Aims

- To ensure all pupils of all abilities and backgrounds achieve their full potential.
- To establish and maintain a caring and inclusive ethos, with the wellbeing of all a priority.
- To support all our learners in becoming ambitious, capable learners who are ready to learn throughout their lives.
- To enable our children to be enterprising, creative contributors who are ready to play a full part in their education, life and work.
- To support all children to become ethical, informed citizens who are ready to become citizens of Wales and the world, and who have respect for each other.
- To ensure children develop into healthy, confident individuals who are ready to lead fulfilling lives as valued members of our society.

To achieve our aims we will:

- Listen to our children and provide opportunities for pupil participation in school life
- Provide a stimulating, caring and safe environment, both inside and out
- Provide a versatile curriculum, that is challenging, creative and highly stimulating
- Equip our children with ‘Learning Assets’ : collaborating, researching, communicating, self-managing and thinking. These skills and dispositions will act as important assets to them as learners across the curriculum, in school and beyond.
- Ensure a relevant ‘Pupil Offer’ of experiences and opportunities that is unique to the needs of our learners and learning community.
- Provide an open door policy for parents and carers
- Provide high quality, caring, well trained staff
- Provide opportunities for pupils to work confidently, both independently and collaboratively
- Provide consistent and fair positive behaviour management strategies to ensure a calm working and learning environment
- Provide appropriate and good quality resources to aid teaching
- Provide strong, effective management and leadership
- Celebrate our learners’ successes with our enthusiasm and smiles!

The internet can be a valuable learning and communication tool and is a part of everyday life for our school community. Our aim is to ensure that children and staff are safe, well informed and receive appropriate guidance when using online technologies.

Online Safety Policy

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is 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 made available to staff through SmartLog
- is published on the school website.

Education

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 develop their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be accessible to all, broad, relevant and provide progression.

Responsibilities

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

Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the Online Safety Lead.
- The headteacher and deputy headteacher will 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 is responsible for ensuring that technical staff and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.

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 governor with responsibility for IT who will receive information about online safety incidents and monitoring reports. The governor with responsibility for IT will:

- have meetings with the Online Safety Lead
- receive (collated and anonymised) reports of online safety incidents
- check that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training) is taking place as intended
- report findings and feedback to relevant governors

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

Online Safety Lead

The online safety lead will:

- work closely with the Designated Safeguarding Person (DSP)
- 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 and learners.
- liaise with technical staff and school staff
- meet with the governor with responsibility for IT to discuss current issues and review (anonymised) incidents and if necessary
- attend relevant governing body meetings
- report to senior leadership team
- liaise with the local authority

Designated Safeguarding Person (DSP)

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

Area for Learning and Experience Leads

Leaders of Areas for Learning and Experiences will work with the online safety lead to develop a planned and coordinated online safety education programme. This will be provided through:

- discrete ICT learning and teaching experiences
- the Digital Competence Framework

- personal and social education/sex and relationships education
- assemblies
- relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.
- E-Safety themes explored termly during learning to learn weeks across the school
- Sharing Rogerstone Primary School's Online Agreements with learners (see appendix 2 & 3)

Teaching and support staff

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 and understood the school's Online Safety Policy
- they immediately report any suspected misuse or problem to the designated safeguarding person or online safety lead for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/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
- ensure learners understand and follow the Online Agreements (see appendix 2 & 3)
- they supervise and monitor the use of digital technologies in lessons and other school activities 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
- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies
- they have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Network Manager / Technical staff:

Rogerstone Primary School has a managed ICT service provided by iTeach and it is the responsibility of the school to ensure that iTeach carries out all the e-Safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the school's Online Safety Policy and procedures.

iTeach is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that 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 e-Safety Policy / Guidance that may apply. (recommended web filtering standards for schools in Wales June 15)
- that 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 technical and communications systems is regularly monitored in order that any misuse/attempted misuse can be reported to the online safety lead for investigation and action
- that they collaborate with the school's Senior Information Risk Owner (School Information Security Policy)
- 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
- all children (Y2 and above) will be provided with a username and secure password for Google Drive. The ICT leader will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to use a generic password provided by the teacher.
- all children in FPh will be provided with a class username and secure password for GoogleDrive.
- the "master / administrator" passwords for the school ICT system, used by iTeach, must also be available to the school.
- 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.

Learners

- are responsible for using the school digital technology systems in accordance with the school's Online Agreements (see appendix 2 & 3)

- 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 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

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

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:

- providing them with a copy of the learners' online agreement
- publish information about appropriate use photos/videos and social media relating to posts concerning the school

Parents and carers will be encouraged to support the school in reinforcing the online safety messages provided to learners in school.

Acceptable use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below. Key messages are shared with the learners through our Online Agreements (see appendix 2 & 3). Learners will be introduced to and reminded of the agreements during lessons, learning to learn weeks, digital leader activities, assemblies and displays in class and around the school.

User actions		Acceptable	Acceptable at certain time	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images – the making, production or distribution of indecent images of children, contrary to The Protection of Children Act 1978 N.B. Schools should refer to guidance about dealing with nudes and semi-nudes being shared.					X
	grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003					X
	possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character), contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	promotion of extremism or terrorism				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act (1990): ● Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) ● Gaining unauthorised access to school networks, data and files, through the use of computers/devices ● Creating or propagating computer viruses or other harmful files ● Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) ● Disable/Impair/Disrupt network functionality through the use of computers/devices ● Using penetration testing equipment (without relevant permission) The school will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to						X

prevent learners becoming involved in cyber-crime and harness their activity in positive ways – further information here.					
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information, (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Online gaming (educational)	x				
Online gaming (non educational)				x	
Online gambling				x	
Online shopping/commerce		x			
File sharing	x				
Use of social media		x			
Use of messaging apps		x			
Use of video broadcasting		x			

Staff and other adults

	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission
Mobile phones may be brought to school	x						
Use of mobile phones in lessons		x					
Use of mobile phones in social time	x						
Taking photos on mobile phones/cameras			x				
Use of other mobile devices, e.g. tablets, gaming devices	x						

Use of personal e-mail addresses in school, or on school network				x			
Use of school e-mail for personal e-mails				x			
Use of messaging apps				x			
Use of social media				x			
Use of blogs				x			

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.
- 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 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 digital citizenship and 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.

Reporting and responding

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 (see appendix 1), 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
- 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 school 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 reporting or affected by an online safety incident
- incidents should be logged
- 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
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
  - *the online safety lead and senior leaders 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*

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:

Learner actions

Incidents	Refer to class teacher	Refer to Headteacher/ Deputy Head	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			
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		
Continued infringements of the above, following previous warnings or sanctions.		x			x			x

Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		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	
Deliberately accessing or trying to access offensive or pornographic material.		x				x		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	x						x	

Staff Actions

Incidents	Refer to line manager	Refer to Headteacher	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		X	X	X				

section on unsuitable/inappropriate activities)								
Inappropriate personal use of the internet/social media/personal e-mail		x				x		x
Unauthorised downloading or uploading of files.		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
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
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x				x		x
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature.		x				x		x
Using personal e-mail/social networking/messaging to carrying out digital communications with learners and parents/carers		x				x		x
Actions which could compromise the staff member’s professional standing		x				x		x
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		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		
Deliberately accessing or trying to access offensive or pornographic material		x				x		x
Breaching copyright or licensing regulations.		x				x		x
Continued infringements of the above, following previous warnings or sanctions.		x						x

Training

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered will be an integral part of the school's annual safeguarding and data protection training for all staff. The Online Safety Lead and Designated Safeguarding Person will receive regular updates through training events or materials (e.g. Hwb Keeping safe online training events, from the Regional Consortium/SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations. The Online Safety Lead, or other nominated person, will provide advice/guidance/training to individuals as required.

Governors
Governors should take part in online safety training/awareness sessions. 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 (this may include attendance at assemblies/lessons).

Families
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 seek to provide information and awareness to parents and carers through:

- communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- letters, newsletters, website, learning platform, Hwb
- high profile events/campaigns e.g. Safe Internet Day
- reference to the relevant web sites/publications, e.g. Hwb Keeping safe online, www.saferinternet.org.uk/ www.childnet.com/parents-and-carers
- sharing good practice with other schools in clusters and or the local authority

Technology

ITeach are responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible. They will ensure:

- the school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the Welsh Government Recommended

web filtering standards for schools and the UK Safer Internet Centre Appropriate filtering.

- internet access is filtered for all users
- illegal content (e.g. child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated (n.b. additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet - see Appendix for information on 'appropriate filtering/monitoring')
- there are established and effective routes for users to report inappropriate content
- there *is a clear process in place to deal with requests for filtering changes*
- *the school has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users: staff/learners, etc.)*
- *younger learners will use child friendly/age appropriate search engines e.g. SWGfL Swiggle*
- there is an appropriate and balanced approach to providing access to online content according to role and/or need
- filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.
- where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- the system manages access to content through non-browser services (e.g. apps and other mobile technologies)

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

Monitoring

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- *pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.*

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

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

Technical Security

Schools should read the guidance available in the Hwb tools and services - Trust Centre

- school technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- there will be regular reviews and audits of the safety and security of school technical systems
- 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, (this is good practice in helping to prevent loss of data from ransomware attacks)
- 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 Network Manager (or other person) and will be reviewed, at least annually, by the Online Safety Group (or other 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. Sharing of passwords or ID 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 system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by iTeach who will keep an up to date record of users and their usernames (see section on password generation in 'Technical security policy template' in the Appendix)
- passwords should be long.
- records of learner usernames and passwords can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.
- iTeach 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.
- removable media (e.g. memory sticks/CDs/DVDs) will not be used by users on school devices.

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/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.

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

- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images. Staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes
- care should be taken when taking digital/video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. Permission is not required for images taken solely for internal purposes
- 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

Online Publishing

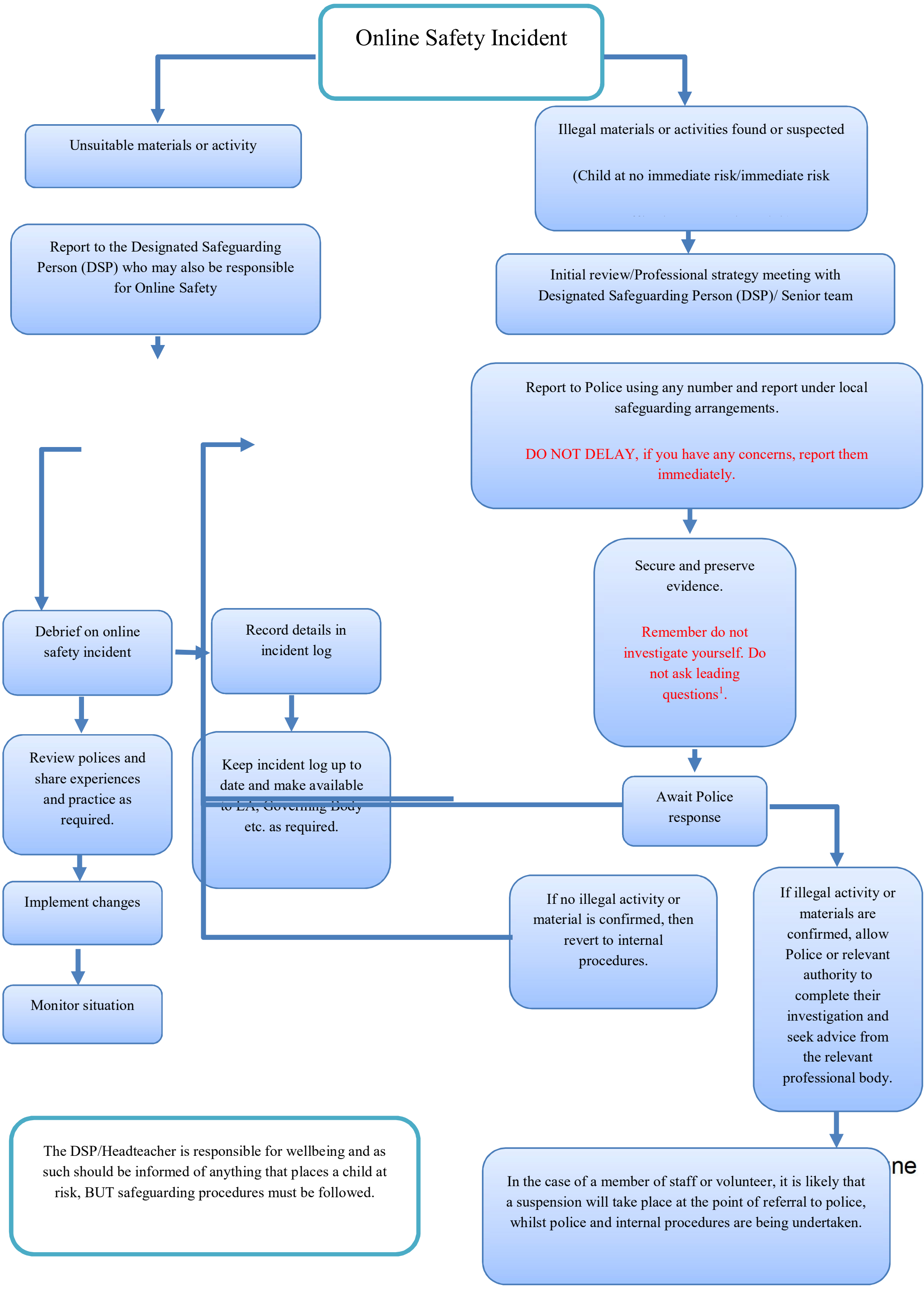
The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media
- Online newsletters
- Texts
- Letters

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

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

Appendix 1



Online Safety Incident

Unsuitable materials or activity

Report to the Designated Safeguarding Person (DSP) who may also be responsible for Online Safety

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Keep incident log up to date and make available to LA, Governing Body etc. as required.

Implement changes

Monitor situation

Illegal materials or activities found or suspected

(Child at no immediate risk/immediate risk

Initial review/Professional strategy meeting with Designated Safeguarding Person (DSP)/ Senior team

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not ask leading questions[1].

Await Police response

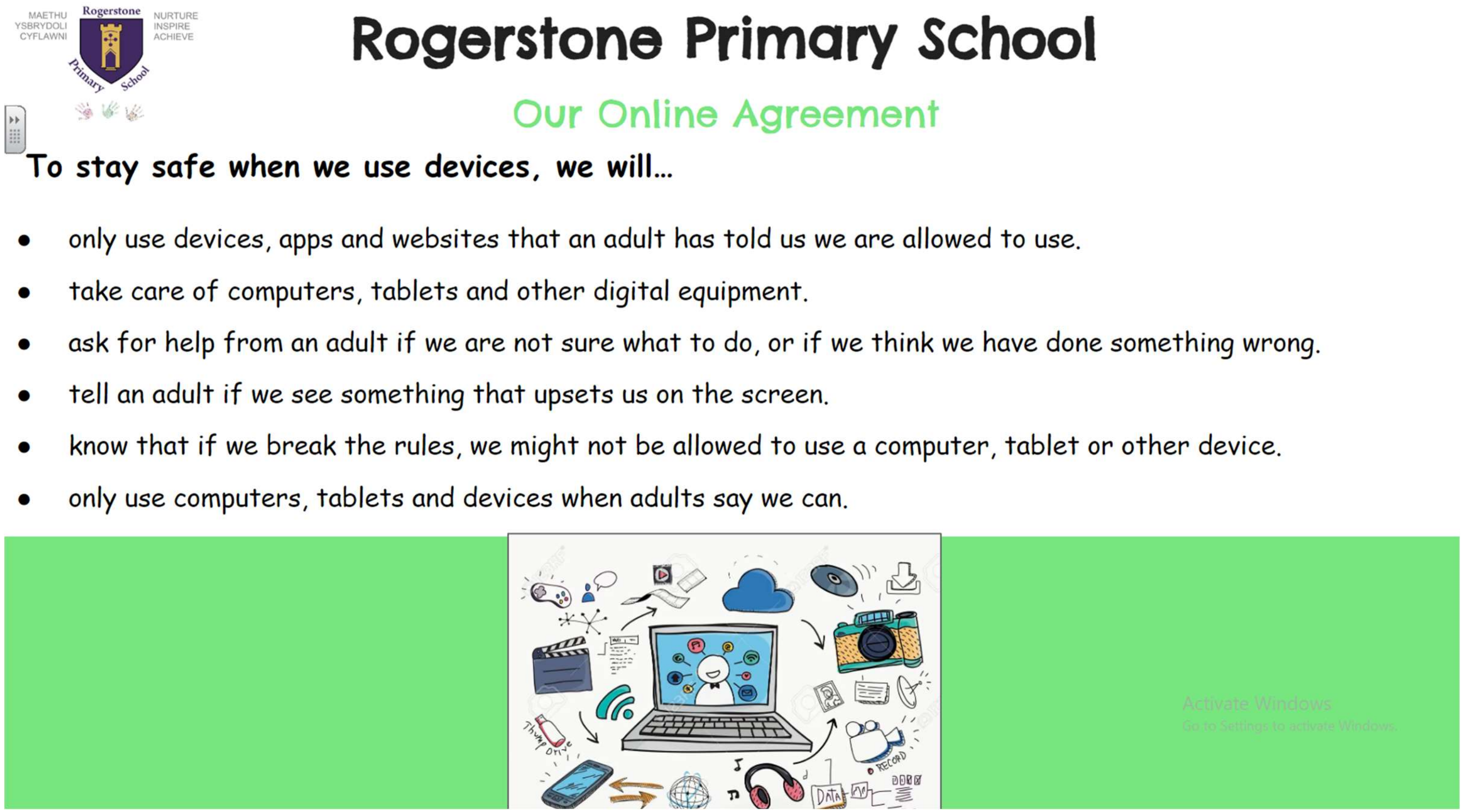
If no illegal activity or material is confirmed, then revert to internal procedures.

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

The DSP/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Appendix 2 - Foundation Phase Online Agreement



MAETHU
YSBRYDOLI
CYFLAWNI

Rogerstone Primary School

NURTURE
INSPIRE
ACHIEVE

Rogerstone Primary School

Our Online Agreement

To stay safe when we use devices, we will…

- only use devices, apps and websites that an adult has told us we are allowed to use.
- take care of computers, tablets and other digital equipment.
- ask for help from an adult if we are not sure what to do, or if we think we have done something wrong.
- tell an adult if we see something that upsets us on the screen.
- know that if we break the rules, we might not be allowed to use a computer, tablet or other device.
- only use computers, tablets and devices when adults say we can.

Appendix 3 - KS2 Online Agreement

Rogerstone Primary School

MAETHU
YSBRYDOLI
CYFLAWNI

Rogerstone Primary School

NURTURE
INSPIRE
ACHIEVE

KS2 Online Agreement

We have an online agreement to make sure that learners when we will be responsible users and stay safe while using digital technologies. We will understand good online behaviours that we can use in school, but also outside school.

We agree to…

- understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly
- only visit internet sites that adults have told me are safe to visit
- keep our usernames and password safe and not share it with anyone else
- not share personal information about myself or others when online
- immediately tell an adult if we see anything that makes us feel uncomfortable when we are online.
- handle all the devices carefully and only use them if we have permission.
- not alter the settings on any devices or try to install any software or programmes.
- tell an adult if a device is damaged or if anything else goes wrong.
- only use the devices to do things that I am allowed to do.
- act as I expect others to act toward me when online
- not copy anyone else's work or files without their permission.
- be polite and responsible when we communicate with others and we appreciate that others may have different opinions to me.
- not take or share images of anyone without their permission.