

# CRYNALLT PRIMARY SCHOOL

## YSGOL GYNRADD CRYNALLT

Head Teacher / Pennaeth: MRS N BRIDGMAN

Telephone – 01639 635256

E-mail [\\_office@crynalltprimary.npt.school](mailto:_office@crynalltprimary.npt.school)

Website – <https://crynallt-primary-school.j2bloggy.com>



### Online Safety Policy

Chair of Governors: Dr Kim Jenkins

Signed: 

Date:







Approved:

Reviewed:

## Contents

Development, monitoring and review of the Policy  
Schedule for development, monitoring and review

What is Online Safety?  
Why is Internet Use Important?

What are the Dangers?

Roles and Responsibilities

- Governors
- Headteacher and Senior Leaders
- Online Co-ordinator
- County Managed Service Provider
- Teaching and Support Staff
- Designated senior person
- Online safety group
- Learners
- Parents / Carers
- Community Users

Policy Statements

- Education – Students / Pupils
- Education – Parents / Carers
- Education – The Wider Community
- Education and training – Staff / Volunteers
- Training – Governors
- Use of digital and video images
- Data protection
- Communications
- User Actions - unsuitable / inappropriate activities
- Responding to incidents of misuse



## Development/Monitoring/Review of this Policy

This online safety policy has been developed by a working group made up of:

- *Acting Headteacher (Mrs Bridgman)*
- *Acting Deputy Headteacher (Miss L Williams)*
- *Senior leaders (Mrs Neal, Mr J. Bridgman, Mr M. Fitchett, Miss L. Williams)*
- *Online safety officer (Mrs Neal)*
- *Staff – including practitioners and support staff*
- *Chair of Governors (Mr P. Rees)*
- *Parents and Carers*
- *Pupils (Digital Champions)*

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

### Schedule for Development/Monitoring/Review

This online safety policy was approved by the <i>Governing body/governors subcommittee</i> on:	
The implementation of this online safety policy will be monitored by the:	<i>Online Safety Officer Child Protection Officer Online Safety Committee</i>
Monitoring will take place at regular intervals:	<i>Annually</i>
The <i>Governing Body/governors subcommittee</i> 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:	<i>Annually</i>
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:	<i>Spring Term 2023</i>
Should serious online safety incidents take place, the following external persons/agencies should be informed:	<i>LA ICT manager LA Safeguarding officer Police</i>

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Monitoring logs of internet activity (including sites visited)*
- *Surveys/questionnaires of*
  - *Learners*
  - *Parents and Carers*
  - *Staff*



## Introduction

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.

## What is Online Safety?

Online Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and should actively encourage responsible and safe use of their online experiences. The school's Online Safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Anti-Bullying, Child Protection, Curriculum, Data Protection and Security.

## Why is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

Many pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

## What are the Dangers?

Some of the dangers children may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files



## Crynallt Primary School – Online Safety Policy

- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate them completely. It is therefore essential, through good educational provision to build pupils' resilience to the threats to which they may be exposed, so that they have the confidence and skills to face and deal with these dangers.

The following policy explains the necessary safeguards that we have put in place to manage and reduce these risks.

## 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 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:

- Termly meetings with the online safety co-ordinator
- regular monitoring of online safety incident logs
- 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 co-ordinator
- 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 is responsible for ensuring that the online safety co-ordinator 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 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 will receive Termly monitoring reports from the online safety co-ordinator.

### Online Safety Co-ordinator:

The online safety co-ordinator

- leads the online safety group



## Crynalit Primary School – Online Safety Policy

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- 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
- 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
- attends relevant meeting/sub-committee of governors
- reports regularly to headteacher/senior leadership team

### County Managed Service Provider:

The managed service provider is responsible for ensuring:

- that the school 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 online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that 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
- that the use of the internet is regularly monitored in order that any misuse/attempted misuse can be reported to the headteacher and online safety co-ordinator for investigation/action/sanction
- that (if present) monitoring software/systems are implemented and updated as agreed in school policies
- that the 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:

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 and/or online safety co-ordinator 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



## Crynalit Primary School – Online Safety Policy

### Designated Senior Person:

The designated senior 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
- cyber-bullying

### Online safety group:

The online safety group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the online safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the online safety group will assist the online safety co-ordinator with:

- the production/review/monitoring of the school online safety policy/documents.
- the production/review/monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/incident logs where possible
- consulting stakeholders – including parents/carers and the learners about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe Cymru self-review tool

### Learners:

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement (AUA)
- 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 cyber-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 understand these issues through *parents' evenings, newsletters, letters, website, Hwb, learning platform and information about national/local online safety campaigns/literature.*



## Crynallt Primary School – Online Safety Policy

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' sections of the website, Hwb, learning platform and online learner records



## Policy Statements

### Education – learners

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, (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

The school will 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 web sites/publications*

### 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



## 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.
- *The online safety co-ordinator will receive regular updates through attendance at external training events, and by reviewing guidance documents released by relevant organisations.*
- *This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.*
- *The online safety co-ordinator 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:

- Attendance at training provided by the Local Authority/National Governors Association /or other relevant organisation,
- Participation in school training/information sessions for staff or parents

## Technical – infrastructure/equipment, filtering and monitoring

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. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- 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 must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the Online Safety Coordinator who will have access to an up to date record of users. Users are responsible for the security of their username and password and will be required to change their password on a regular basis or when they feel their security has been compromised.
- The “master/administrator” passwords for the school digital systems, used by the network manager must also be available to the headteacher or other nominated senior leader and kept in a secure place, (e.g. school safe).
- 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 by the service provider. There is a clear process in place to deal with requests for filtering changes



## Crynallt Primary School – Online Safety Policy

- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different groups of users: staff/learners/administrators, etc.).
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- 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 by the service provider. The school infrastructure and individual workstations are protected by up to date virus software.

### 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 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 email 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 school allows:

	School Devices	Personal Devices	
	School owned for multiple users	Pupil owned	Staff owned
Allowed in school	Yes	No	Yes
Full network access	Yes		
Internet only			
No network access			

### Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and



## Crynalit Primary School – Online Safety Policy

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 cyberbullying 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.*
- *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' names will not be used anywhere on a website in association with photographs.*
- *Written permission from parents or carers will be obtained before photographs of learners are published on the school website*

## Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- 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.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the privacy notice and lawfully processed in accordance with the conditions for processing.



## Crynalit Primary School – Online Safety Policy

- It has a data protection policy
- It is registered as a data controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed/identified - senior information risk officer (SIRO) and information asset owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear data protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage/cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

### 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.
- 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.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

## Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:



## Communication Technologies

	Staff & other adults				Learners			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school								
Use of mobile phones in lessons for educational purposes								
Use of mobile phones in social time								
Taking photos on mobile phones/cameras								
Use of other mobile devices e.g. tablets, gaming devices								
Use of personal email addresses in school, or on school network								
Use of school email for personal emails								
Use of messaging apps								
Use of social media								
Use of blogs								

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

- The official school email service (Hwb) may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report to the Headteacher – 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 (email, chat, learning platform, etc.) must be professional in tone and content.
- *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 email addresses should be used to identify members of staff.*

### Social media

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



## Crynalit Primary School – Online Safety Policy

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; 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, including
- 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

Unsuitable/Inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in, or out of, school when using school equipment or systems. The school policy restricts usage as follows:



## User Actions

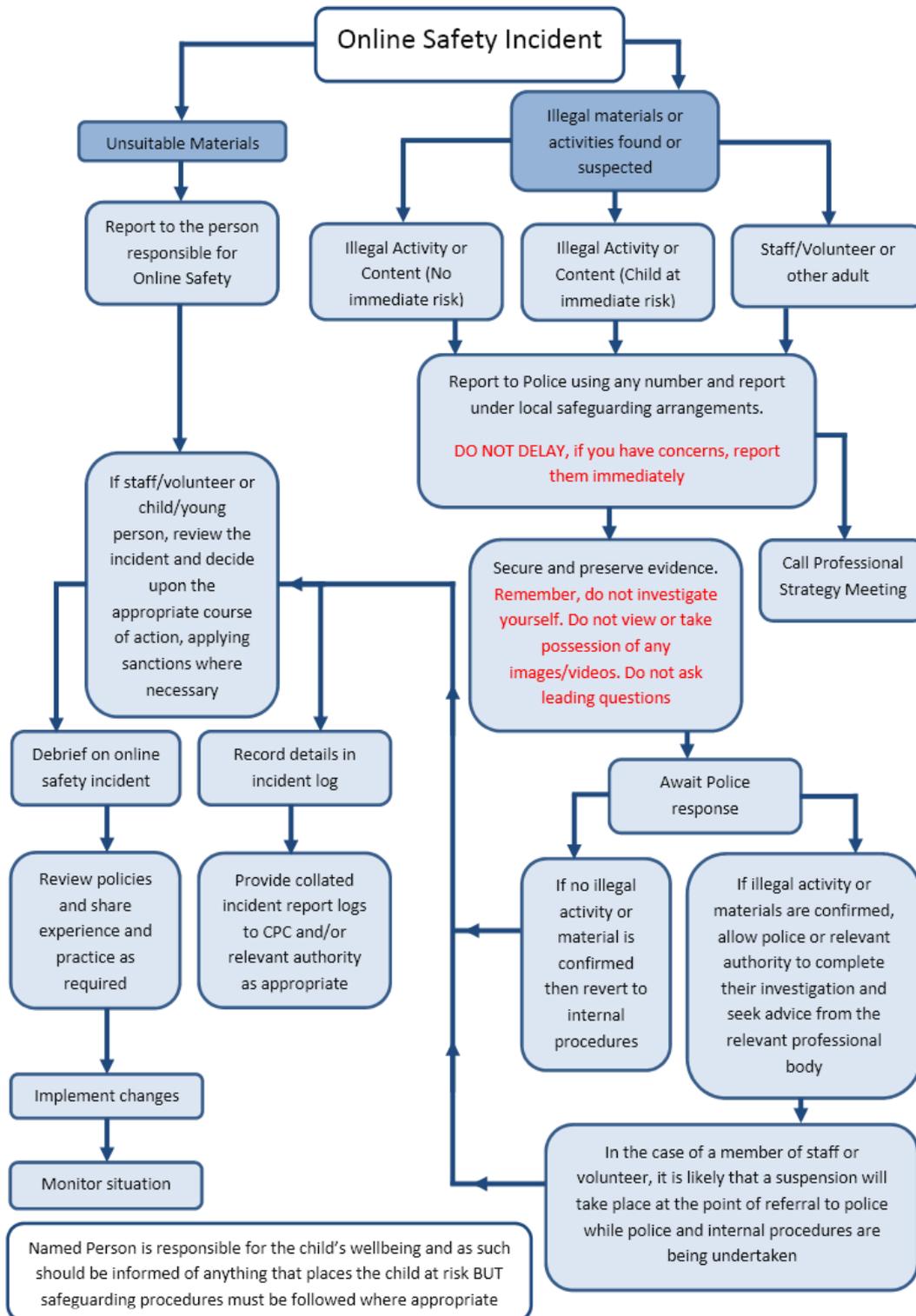
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children, contrary to The Protection of Children Act 1978					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		
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 (for personal reasons)				X		
File sharing	X					
Use of social media				X		
Use of messaging apps (social)				X		
Use of video broadcasting, e.g. YouTube			X			

## Responding to incidents of misuse

### Illegal Incidents

## Crynalit Primary School – Online Safety Policy

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the flowchart (below) for responding to online safety incidents and report immediately to the police.



### Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless, irresponsible or, very rarely, through deliberate misuse.



## Crynalit Primary School – Online Safety Policy

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff/volunteer 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. 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
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by local authority or national/local organisation (as relevant).
  - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the police immediately. Other instances to report to the police 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
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

### 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	Refer to Police	Refer to technical support staff for action re filtering/security	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction eg. 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					
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 email	X						X	
Unauthorised downloading or uploading of files	X						X	
Allowing others to access school network by sharing username and passwords	X	X		X	X	X	X	X
Attempting to access or accessing the school network, using another learners' account	X						X	X
Attempting to access or accessing the school network, using the account of a member of staff	X	X		X	X	X	X	X
Corrupting or destroying the data of other users	X	X		X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X		X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X		X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X					X	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	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 email	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. holding or transferring data in an insecure manner	X	X	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 email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X		X		
Using personal email/social networking/messaging to carrying out digital communications with learners	X	X						
Actions which could compromise the staff member's professional standing	X	X						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X						
Using proxy sites or other means to subvert the school's filtering system	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	X	X	X	X
Breaching copyright or licensing regulations	X	X						
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X



# Appendix

## Appendices – Section A - Acceptable use agreement

- A1 Learner Acceptable use agreement template (younger children)
- A2 Learner Acceptable use agreement template (older children)
- A3 Staff and Volunteers Acceptable use agreement template
- A4 Parents /Carers Acceptable use agreement template

## Appendices – Section B – Supporting documents and links

- C1 Reporting log template
- C2 Summary of legislation
- C3 Office 365 – further details
- C4 Links to other organisations and documents
- C5 Glossary of terms



# Appendices

## Section A

### Acceptable use agreement



## A1 Acceptable Use Agreement (Lower School)

This is how we stay safe when we use computers:

- I will ask a teacher or another adult from the school if I want to use the computers
- I will only use activities that a teacher or another adult from the school has told or allowed me to use.
- I will take care of the computer and other equipment
- I will ask for help from a teacher or another adult from the school if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or another adult from the school if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer/tablet.

Signed (child): .....

Signed (parent): .....



## A2 Acceptable Use Agreement (Upper School)

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.)
- 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 devices are to be used for learning and will ask permission to use them for recreational use
- I will not download anything without permission
- I will ask for permission to share files

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 their 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 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 immediately report any damage or faults of 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

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 cyber-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



## Crynalit Primary School – Online Safety Policy

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.

**Please complete the sections 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.**

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: .....

Group/Class .....

Signed: .....

Date: .....



## Crynalit Primary School – Online Safety Policy

### 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.



## Crynalit Primary School – Online Safety Policy

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 their permission and in accordance with the schools' policy on the use of digital/video images. I will only use my personal equipment to record these images, if I have permission to do so. Where these images are published, (e.g. on the school website/learning platform) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner. Staff should be made aware of the risks attached to using their personal email addresses/mobile phones/social networking sites for such communications)
- 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 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:



## Crynallt Primary School – Online Safety Policy

- 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 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: .....



# A4 Parent/Carer Staff and Volunteer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide 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 safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people 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.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their online behaviour.

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. A copy of the Learner Acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the schools' work.

Permission Form

Parent/Carers Name:..... Learner's Name .....

As the parent/carers of the above learner(s), I give permission for my son/daughter to have access to the internet and to digital technology systems at school.

Either: (KS2 and above)

- *I know that my son/daughter has signed an acceptable use agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.*

Or: (Foundation)

- *I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.*
- I understand that the school will take every reasonable precaution, including applying monitoring and filtering systems, to ensure that young people will be safe when they use the internet and digital technology systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my son's/daughter's activity on the digital technology systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed ..... Date: .....

Use of Digital/Video Images



## Crynallt Primary School – Online Safety Policy

The use of digital/video images plays an important part in learning activities. Learners and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,

The school will comply with the Data Protection Act and request parents/carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

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.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

### Digital/Video Images Permission Form

Parent/Carers Name: .....

Learners Names: .....

As the parent/carer of the above learner(s), I agree to the school taking and using digital/video images of my child/children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Yes/No
Yes/No

Signed ..... Date: .....

Signed ..... Date: .....

Name ..... Signed ..... Date: .....



# Section C

# C1 Reporting Log Template

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

## C2 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.

### Computer Misuse Act 1990

This Act makes it an offence to:

- erase or amend data or programs without authority;
- obtain unauthorised access to a computer;
- “eavesdrop” on a computer;
- make unauthorised use of computer time or facilities;
- maliciously corrupt or erase data or programs;
- deny access to authorised users.

### Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- fairly and lawfully processed.
- processed for limited purposes.
- adequate, relevant and not excessive.
- accurate.
- not kept longer than necessary.
- processed in accordance with the data subject’s rights.
- secure.
- not transferred to other countries without adequate protection.

### Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

### Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent,

obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

## Malicious Communications Act 1988

It is an offence to send an indecent, grossly offensive, or threatening letter, electronic communication or other article to another person. It is also an offence to send information which is false and known or believed to be false by the sender.

## Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Where the system controller has given express consent monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- establish the facts;
- ascertain compliance with regulatory or self-regulatory practices or procedures;
- demonstrate standards, which are or ought to be achieved by persons using the system;
- investigate or detect unauthorised use of the communications system;
- prevent or detect crime or in the interests of national security;
- ensure the effective operation of the system.
- monitoring but not recording is also permissible in order to:
- ascertain whether the communication is business or personal;
- protect or support help line staff

## Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

## Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

## Criminal Justice & Public Order Act 1994/Public Order Act 1986

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

## Racial and Religious Hatred Act 2006/Public Order Act 1986

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

## Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

## Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18.. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence is liable to imprisonment for a term of not more than 10 years, or to a fine or to both.

## Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

## Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

## Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

## Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- the right to a fair trial
- the right to respect for private and family life, home and correspondence
- freedom of thought, conscience and religion
- freedom of expression
- freedom of assembly
- prohibition of discrimination
- the right to education
- the right not to be subjected to inhuman or degrading treatment or punishment

The school is obliged to respect these rights and freedoms, but should balance them against those rights, duties and obligations, which arise from other relevant legislation.

## The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carers to use Biometric systems

## C3 Office 365 – further information

## Where is the data stored?

Data for UK Schools is all hosted within the EU. The primary Microsoft data centre we host the service in is located in Dublin and the fail-over is to Amsterdam.

## How often is the data backed up?

The idea of “back up” is very different with Office365 than with traditional locally hosted services. We use a network of globally redundant data centres and replicate data on multiple servers across the two data centres. Any one time we keep 3 copies of schools data across the two data-centres mentioned (Dublin & Amsterdam).

## Does the email service provider have a clear process for recovering data?

Yes. Users themselves can recover data for 30 days after deleting an item. Administrators then have a further 30 days once the item is deleted from the deleted-items folder. There are also additional paid-for archiving services available with Office365, but with a 25GB inbox per person the pressure on users to archive email is not as great compared to existing email systems.

## How does the email provider protect your privacy?

3 key things: No advertising, no “mingling” of Office 365 data with our consumer services (such as Hotmail) and full data-portability, in case you ever want to leave the service.

## Who owns the data that you store on the email platform?

Schools own the data. Microsoft does not. You own your data, and retain all rights, title and interest in the data you store with Office 365. You can download a copy of all of your data at any time and for any reason, without any assistance from Microsoft.

## Who has access to the data?

By default no one has access to customer data within the Office 365 service. Microsoft employees who have completed appropriate background checks and have justified need can raise an escalation for time-limited access to Customer data. Access is regularly audited, logged and verified through the ISO 27001 Certification.

As detailed in a recent accreditation submission to the UK Government, any organisation that specify “UK” as their country during tenant creation will be provisioned and data stored within the EU datacenters (Dublin and Amsterdam).

Microsoft has been granted accreditation up to and including the UK government’s “Impact Level 2” (IL2) assurance for Office 365. As of February 2013 Microsoft are the only major international public cloud service provider to have achieved this level of accreditation and, indeed, it is the highest level of accreditation possible with services hosted outside of the UK (but inside of the EEA).

Schools may wish to consider the extent to which applicable laws in the US – which apply to services operated by companies registered in the US, e.g. Microsoft and Google – affect the suitability of these services. For example the US Patriot Act provides a legal means through which law enforcement agencies can access data held within these services without necessarily needing the consent or even

the knowledge of the customer. Whilst SWGfL doesn't intend to put anyone off getting value from these beneficial services we feel it's only right to share what we know about them.

Is personal information shared with anyone else?

No personal information is shared.

Does the email provider share email addresses with third party advertisers? Or serve users with ads?

No. There is no advertising in Office365.

What steps does the email provider take to ensure that your information is secure?

Microsoft uses 5 layers of security - data, application, host, network and physical. You can read about this in a lot more detail [here](#).

Office365 is certified for ISO 27001, one of the best security benchmarks available across the world. Office 365 was the first major business productivity public cloud service to have implemented the rigorous set of physical, logical, process and management controls defined by ISO 27001.

EU Model Clauses. In addition to EU Safe Harbor, Office 365 is the first major business productivity public cloud service provider to sign the standard contractual clauses created by the European Union ("EU Model Clauses") with all customers. EU Model Clauses address international transfer of data.

Data Processing Agreement. Microsoft offers a comprehensive standard Data Processing Agreement (DPA) to all customers. DPA addresses privacy, security and handling of customer data. Our standard Data Processing Agreement enables customers to comply with their local regulations. Visit [here](#) to get a signed copy of the DPA.

How reliable is the email service?

There is a 99.9% uptime commitment with financially-backed SLA for any paid-for services in Office365 (though most schools will be using 'free' services and therefore will not receive the financially backed SLA).

What level of support is offered as part of the service?

Microsoft offer schools direct telephone support 24/7 for IT administrators and there is also a large range of online help services, which you can read about [here](#). Our recommendation is that schools use a Microsoft partner or support organisation with industry specific expertise in cloud services for schools.

## C4 Links to other organisations or documents

These may help those who are developing or reviewing an online safety policy.

## UK Safer Internet Centre

- [Safer Internet Centre](#)
- [South West Grid for Learning](#)
- [Childnet](#)
- [Professionals Online Safety Helpline](#)
- [Internet Watch Foundation](#)

## CEOP

- <http://ceop.police.uk/>
- [ThinkUKnow](#)

## Others

- INSAFE - <http://www.saferinternet.org/ww/en/pub/insafe/index.htm>
- UK Council for Child Internet Safety (UKCCIS) - [www.education.gov.uk/ukccis](http://www.education.gov.uk/ukccis)
- Netsmartz - <http://www.netsmartz.org/index.aspx>

## Cyberbullying

- Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>
- Scottish Government - [Better relationships, better learning, better behaviour](#)
- [Welsh Government – Respecting Others](#)
- Anti-Bullying Network - <http://www.antibullying.net/cyberbullying1.htm>
- Cyberbullying.org - <http://www.cyberbullying.org/>
- Enable – EU funded anti-bullying project - <http://enable.eun.org/>

## Sexting

- [UKCCIS - Sexting in schools and colleges: responding to incidents and safeguarding young people](#) (to be added to both language versions)
- [UKSIC – Responding to and managing sexting incidents](#)

## Social Networking

- Digizen – [Social Networking](#)
- [SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people](#)
- [Connectsafely Parents Guide to Facebook](#)

- [Facebook Guide for Educators](#)

## Curriculum

- [SWGfL Online Safety Resource \(accessed through Hwb\)](#)
- Alberta, Canada - [digital citizenship policy development guide.pdf](#)
- Teach Today - [www.teachtoday.eu/](http://www.teachtoday.eu/)
- Insafe - [Education Resources](#)

## Mobile Devices/BYOD

Cloudlearn Report [Effective practice for schools moving to end locking and blocking](#)  
NEN - [Guidance Note - BYOD](#)

## Data Protection

- Information Commissioners Office:
  - [Your rights to your information – Resources for Schools - ICO](#)
  - [ICO pages for young people](#)
  - [Guide to Data Protection Act - Information Commissioners Office](#)
  - [Guide to the Freedom of Information Act - Information Commissioners Office](#)
  - [ICO - Guidance we gave to schools - September 2012 \(England\)](#)
  - [ICO Guidance on Bring Your Own Device](#)
  - [ICO Guidance on Cloud Computing](#)
  - [Information Commissioners Office good practice note on taking photos in schools](#)
  - [ICO Guidance Data Protection Practical Guide to IT Security](#)
  - [ICO – Think Privacy Toolkit](#)
  - [ICO – Personal Information Online – Code of Practice](#)
  - [ICO – Access Aware Toolkit](#)
  - [ICO Subject Access Code of Practice](#)
  - [ICO – Guidance on Data Security Breach Management](#)
- SWGfL - [Guidance for Schools on Cloud Hosted Services](#)
- LGfL - Data Handling Compliance Check List
- NEN - [Guidance Note - Protecting School Data](#)

## Professional Standards/Staff Training

- Kent - Safer Practice with Technology
- Childnet/TDA - Social Networking - a guide for trainee teachers & NQTs
- Childnet/TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
- UK Safer Internet Centre Professionals Online safety Helpline

## Infrastructure/Technical Support

- Somerset - [Questions for Technical Support](#)
- NEN - [Guidance Note - esecurity](#)

## Working with parents and carers

- [Connect Safely - a Parents Guide to Facebook](#)
- Vodafone Digital Parents Magazine
- Childnet Webpages for Parents & Carers
- Get Safe Online - resources for parents
- [Teach Today - resources for parents workshops/education](#)
- The Digital Universe of Your Children - animated videos for parents (Insafe)
- Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
- Insafe - A guide for parents - education and the new media
- [Internetmatters.org](#)

## Research

- [EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011](#)
- [Futurelab - "Digital participation - its not chalk and talk any more!"](#)

## C5 Glossary of terms

AUA	Acceptable use agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online safety Institute
EA	Education Authority
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational Online safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting.
WAP	Wireless Application Protocol

Copyright of the SWGfL School Online safety policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in October 2014. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.