Tre Uchaf Primary School

Online Safety Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

Development of this Policy

This online safety policy has been written by Craig Jones (ICT Coordinator), Louise Davies (Online Safety Governor) and Christine Hewitt (Head Teacher).

Schedule for Monitoring and Review

This online safety policy was approved by the *Governing Body*	*Written and approved May 2016 and last updated March 2020*
The implementation of this online Safety policy will be monitored by:	*Craig Jones and Louise Davies*
Monitoring will take place at regular intervals:	*Yearly – Spring Term*
The *Governing Body / Governors Sub Committee* will receive a report on the implementation of the online Safety policy at regular intervals:	*Yearly- Spring Term*
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:	*Spring term 2021*

Roles and Responsibilities

The following section outlines the online Safety roles and responsibilities of individuals[1] 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 / Governor's sub-committee* receiving regular information about online Safety incidents and monitoring reports. A member of the Governing Body takes on the role of online Safety Governor[2] (Louise Davies) to include:

- *regular meetings with the online Safety Co-ordinator / Officer*
- *regular monitoring of online Safety incident logs*
- *reporting to relevant Governors / sub-committee / meeting*

Headteacher:

- 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 is delegated to the *online Safety Co-ordinator Craig Jones.*
- The Headteacher and online safety governor 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 Coordinator 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 Senior Management Team will receive regular reports from the online Safety Co-ordinator Craig Jones.*

Online Safety Coordinator

The *online Safety Coordinator*

- leads the online Safety committee

- takes day to day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school online Safety policies and incident log
- 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 training and advice for staff
- liaises with the Local Authority technical staff
- receives reports of online Safety incidents[3] 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 and change control logs
- attends relevant meeting / sub-committee of *Governors*
- reports regularly to Head teacher

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 Policy / Agreement confidentiality agreement
- they report any suspected misuse or problem to the *Headteacher or ICT Coordinator* for investigation
- all digital communications with students / pupils / parents / carers should be on a professional level *and only carried out using official school systems – only Hwb, Class Dojo and Squid.*
  All communications between staff – parent, pupil & governors should be professional in tone and content.
- online Safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-Safety and acceptable use *agreements / policies*
- pupils 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 pupils 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*

Safeguarding Designated Person

The *Safeguarding Designated Person Christine Hewitt* 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 on-line contact with adults and strangers
- potential or actual incidents of grooming
- cyber-bullying

Any incidents should be reported to the Designated safeguarding person or Louise Davies (Deputy Head and Online Safety Governor) in her absence.

Online Safety Governor

The online Safety Governor be responsible for regular reporting to the Governing Body with responsibility for issues regarding online Safety and monitoring the online safety policy including the impact of initiatives in liaison with online safety co-ordinator

The online safety governor will assist the *online Safety Coordinator* with:

- review and monitoring of the school online Safety policy and any documents.
- reviewing the online Safety curricular provision

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

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting 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 and using images and 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.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and 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 and information about national and local online Safety campaigns.* 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 and on-line pupil records
- social media – age guidelines.

Policy Statements

Online Safety should be a focus in all areas of the curriculum and staff should reinforce online Safety messages across the curriculum. The online Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online Safety curriculum should be provided as part of ICT / Computing / PSE / Digital Literacy lessons or other lessons and should be regularly revisited
- Key online Safety messages should be reinforced as part of a planned programme of assemblies.
- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- *Pupils should be helped to understand the need for the Pupil 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 pupils 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 pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*

Education – parents / carers

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

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

- *Curriculum activities*
- *Letters, newsletters, web site*
- *Parents evenings*
- *High profile events / campaigns eg Safer Internet Day*

- *Reference to the relevant web sites / publications eg* https://hwb.wales.gov.uk/ www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education & Training – Staff and 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 onlineSafety training will be made available to staff & students – Hwb Online Safety Zone.
- This will be regularly updated and reinforced. An audit of the online Safety training needs of all staff will be carried out regularly. *It is expected that some staff will identify online Safety as a training need within the performance management/staff appraisal process.*
- All new staff should receive online Safety training as part of their induction programme, ensuring that they fully understand the school online Safety policy and Acceptable Use Agreements.
- *The online Safety Coordinator will receive regular updates through attendance at external training events (eg from Consortium / SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.*
- *This online Safety policy and its updates will be presented to and discussed by staff.*
- *The online -Safety Coordinator will provide advice, guidance and training to individuals as required.*

Training – Governors

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

- Attendance at training provided by the Local Authority, National Governors Association, via HWB online or other relevant organisation (eg SWGfL).
- Participation in school training for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

The school has a managed ICT service provided by the LEA. It is the responsibility of the school to ensure that the managed service provider carries out all the online Safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school online Safety Policy / Acceptable Use Agreements.

The school will be responsible for ensuring that the school 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
- 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 are provided with a username and secure password by ***Hwb and CJ*** *who will keep an up to date record of users and their usernames.*
- The administrator passwords for the school ICT system must also be available to the *Headteacher* .
- 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. (the school will need to decide on the merits of external / internal provision of the filtering service – see appendix). There is a clear process in place to deal with requests for filtering changes (see appendix for more details)
- *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 / pupils / students etc)
- *Staff to inform CJ of any technical incidents to update on incident log.*
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- *An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.*

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils 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 pupils about the risks associated with the taking, using, 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 WAG guidance, 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 GDPR. 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 *students / pupils* 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. Images taken on personal mobile phones will follow our 'tweet and delete' policy. Staff will delete photos once they have served the intention – i.e. uploaded to twitter or school website. Staff are responsible for deleting images automatically uploaded to online storage systems.*
- *Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*
- *Students / pupils must not take, use, share, publish or distribute images of others without their permission*
- *Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.*
- *Pupils' 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 pupils are published on the school website.*
- *Pupils' work can only be published with the permission of the student / pupil and parents or carers.*

Data Protection GDPR

Personal data will be recorded, processed, transferred and made available according to the GDPR guidelines 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".
- 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 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

This is an area of rapidly developing technologies and uses. 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: Discuss in GOVs

Staff & other adults	Students / Pupils

Communication Technologies	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	x							
Use of mobile phones in lessons		x						x
Use of mobile phones in social time	x							x
Taking photos on mobile phones / cameras		x						x
Use of other mobile devices eg tablets, gaming devices		x					x	
Use of personal email addresses in school, or on school network		x						x
Use of school email for personal emails				x				x
Use of messaging apps		x						x
Use of social media		x						x
Use of blogs	x						x	

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. *Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g by remote access).*
- Users must immediately report to the e Safety co-ordinator or 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 pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Whole class and group email addresses may be used at FP, while pupils at KS2 and above will be provided with individual school email addresses for educational use.*
- *Pupils 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 - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out by the General Teaching Council Wales (GTCW) but all adults working with children and young

people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. All staff working at any educational establishment are expected to demonstrate a professional approach and respect for pupils and their families and for colleagues and the learning setting.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: 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 and governors should ensure that:

- No reference should be made in social media to pupils, parents or carers
- They do not take part in social media parent groups
- 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.

Unsuitable / inappropriate activities

Some internet activity e.g accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those 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 school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal

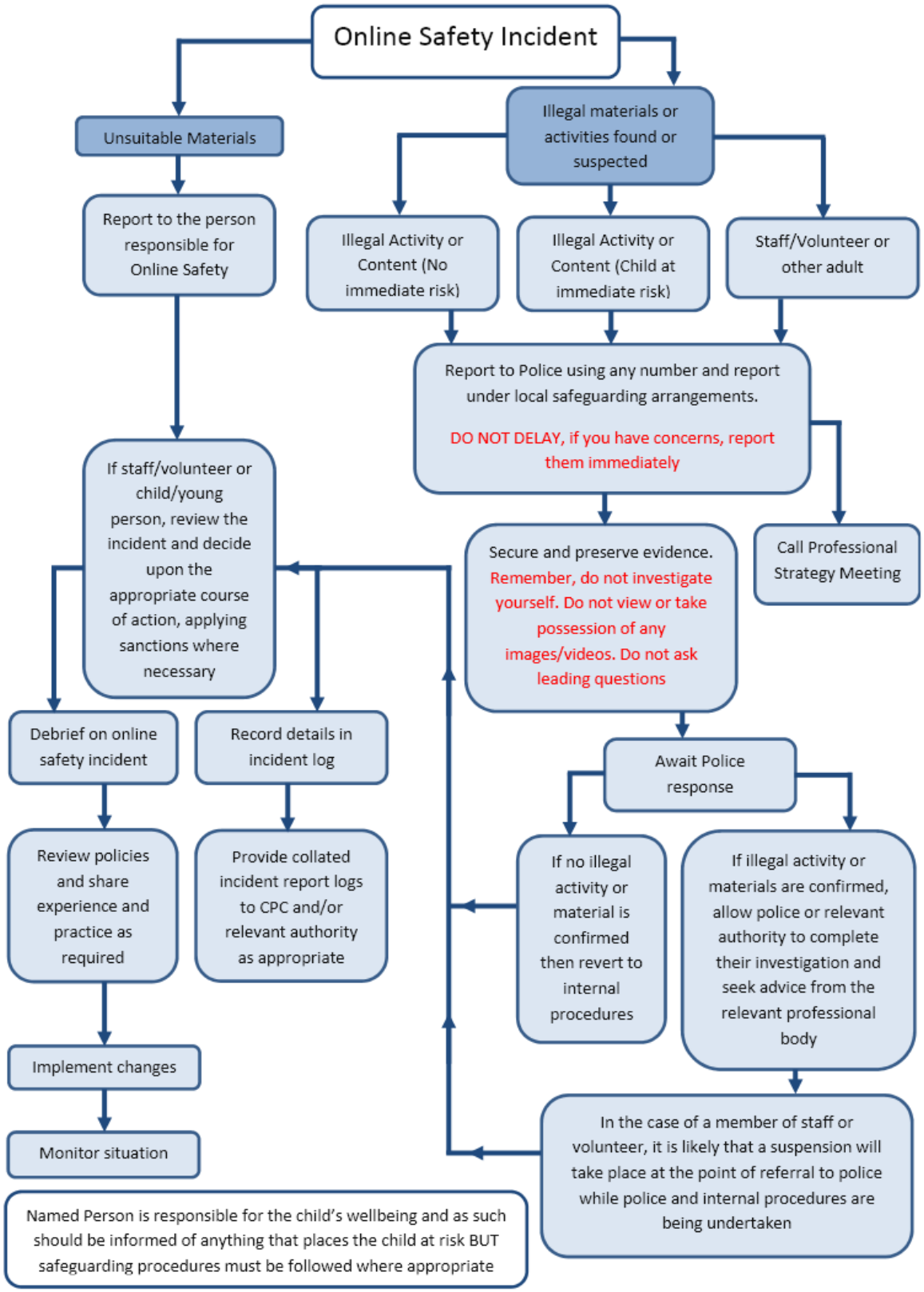
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection 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	
	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 (eg 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	
On-line gaming (educational)	x					
On-line gaming (non educational)		x				
On-line gambling				x		
On-line shopping / commerce			x			
File sharing				x		
Use of social media			x			
Use of messaging apps			x			
Use of video broadcasting eg Youtube			x			

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

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 and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at immediate risk)
Staff/Volunteer or other adult
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have concerns, report them immediately
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Secure and preserve evidence. Remember, do not investigate yourself. Do not view or take possession of any images/videos. Do not ask leading questions
Call Professional Strategy Meeting
Debrief on online safety incident
Record details in incident log
Await Police response
Review policies and share experience and practice as required
Provide collated incident report logs to CPC and/or relevant authority as appropriate
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
Implement changes
Monitor situation
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 while police and internal procedures are being undertaken
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk BUT safeguarding procedures must be followed where appropriate

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 or irresponsible or, very rarely, through deliberate misuse.

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 young people 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 (except in the case of images of child sexual abuse – see below)
- 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
    - 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:

Students / Pupils

Incidents:	Refer to class teacher / tutor	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	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			X			
Unauthorised use of social media / messaging apps / 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	X	X			X			
Attempting to access or accessing the school network, using another student's / pupil's account	X	X			X			
Attempting to access or accessing the school network, using the account of a member of staff	X	X			X			
Corrupting or destroying the data of other users	X	X			X			
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X			X			X
Continued infringements of the above, following previous warnings or sanctions	X	X			X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X			X			X
Using proxy sites or other means to subvert the school's 's filtering system	X	X		X	X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X		X	X			
Deliberately accessing or trying to access offensive or pornographic material	X	X			X			X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X			X		X	

Staff

Incidents:	Refer to Headteacher Principal	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				X
Inappropriate personal use of the internet / social media / personal email	X						
Unauthorised downloading or uploading of files	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		
Careless use of personal data e.g 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	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X						X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	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 '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
Breaching copyright or licensing regulations	X				X		
Continued infringements of the above, following previous warnings or sanctions	X					X	X