



# **Online Safety Policy**

## **Roch CP School**

*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.*

## 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:

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

### Headteacher / Senior Leadership Team (SLT)

- The Headteacher and SLT have a duty of care for ensuring the safety (including online safety) of members of the school community.
- 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, SLT and Designated Safeguarding Persons (DSPs) are responsible for ensuring that staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and ICT coordinator 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 Leadership Team will receive regular monitoring reports from the Online Safety Coordinator and DSPs.

### Online Safety Coordinator

The Online Safety Coordinator has strategic and operational responsibility for online safety.

- leads the online safety committee
- 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
- liaises with Web Trust and DSP in response to alerts generated from pupils' online activity, including searches for inappropriate content such as weapons, violence, sexual content, self-harm, or extremism
- liaises with (school) technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- meets regularly with online safety *Governor* to discuss current issues, review incident logs and if possible, filtering / change control logs
- attends relevant meeting / sub-committee of *Governors*
- reports regularly to Senior Leadership Team

## 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 (AUP / AUA)
- they report any suspected misuse or problem to the Headteacher/SLT/ Online Safety Coordinator for investigation / action
- all safeguarding concerns are recorded promptly on *MyConcern* and are reviewed and acted upon by the DSPs in line with statutory guidance.
- concerns relating to negative behaviour or cyberbullying are logged on *Class Charts* and addressed in accordance with the school's behaviour and anti-bullying procedures.
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the online safety and acceptable use agreements / policies
- students / 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 students / 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

NOTE: It is important to emphasise that these are safeguarding **issues**, not technical issues; the technology provides additional means for safeguarding issues to develop. Some schools may choose to combine the role of DSP and online safety Officer.

The *Safeguarding Designated 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 on-line contact with adults / strangers
- potential or actual incidents of grooming cyber-bullying

## Students / pupils:

- are responsible for using the school digital technology systems in accordance with the Student / 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 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 / Carers

Parents and carers play a crucial role in ensuring that children understand the importance of using the internet and mobile devices safely, responsibly, and appropriately. The school will take every opportunity to support parents and carers in understanding these issues through parents' evenings, newsletters, letters, the school website, and information linked to national and local online safety campaigns.

As part of this approach, a weekly #WebWise Wednesday post will be shared on the school's Facebook page to raise awareness of online safety issues. These posts will provide practical guidance, up-to-date information, and support for parents and carers, as well as suggestions for having positive and meaningful conversations with children about their use of technology. Parents and carers are encouraged to raise any online safety concerns with the school promptly. Parents and carers will be encouraged to work in partnership with the school to promote good online safety practices and to follow school guidelines regarding the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / Hwb and online pupil records
- their children's personal devices in school (where this is permitted).

## Policy Statements

### Education – young people

Whilst regulation and technical solutions are important, they must be balanced with educating pupils to take a responsible and informed approach to using digital technologies. Educating children and young people about online safety is therefore an essential part of the school's wider safeguarding and online safety provision. Pupils need the guidance and support of the school to help them recognise and avoid online safety risks, develop critical thinking skills, and build resilience.

Online safety should be embedded across all areas of the curriculum, with staff consistently reinforcing key messages. The online safety curriculum should be broad, relevant, and progressive, and should provide opportunities for discussion, reflection, and creative activities. Online safety education will be delivered in the following ways:

- A planned online safety curriculum will be provided through **Science and Technology**, the **Digital Competence Framework (DCF)**, **Health and Well-being**, and other relevant lessons, and will be regularly revisited. **Roch CP School follows the Common Sense Education scheme of work, which aligns with the Curriculum for Wales.**
- Key online safety messages will be reinforced through a planned programme of assemblies and tutorial or pastoral activities.
- Pupils' understanding of online safety is monitored through discussion, pupil voice activities, and curriculum evaluation.

- Pupils will be taught, across all lessons, to be critically aware of the content and materials they access online and to evaluate the accuracy and reliability of information.
- Pupils will be taught to acknowledge the sources of information they use and to respect copyright when using material accessed online.
- Pupils will be supported to understand the purpose of the **Acceptable Use Agreement** and encouraged to adopt safe and responsible online behaviours both within and outside of school.
- Staff will act as positive role models in their use of digital technologies, the internet, and mobile devices.
- Where internet use is pre-planned, staff will guide pupils towards websites that have been checked for suitability and ensure clear procedures are in place for dealing with any unsuitable material encountered.
- Where pupils are permitted to search the internet independently, staff will remain vigilant in monitoring the content accessed.

### **Education & Training – Staff / Volunteers:**

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. It is expected that some staff will identify online safety as a training need within the performance management process.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements.
- The Online Safety Coordinator and DCF/Science and tech coordinator 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 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

## Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / 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 students / pupils 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 eg 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 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. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that 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.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

## Data Protection

Personal data will be recorded, processed and stored in accordance with the UK GDPR and the Data Protection Act 2018.

- 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 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

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

- The official school email service may be regarded as safe and secure. Users should be aware that email communications can be monitored. Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems
- Users must immediately report to the nominated person – in accordance with the school policy - the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students / pupils or parents / carers (email, teachers2parents, chat, Hwb 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.
- Students / 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 should ensure that:

- No reference should be made in social media to students / pupils, parents /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.

The school's use of social media for professional purposes will be checked regularly by the Designated Safeguarding Person and ICT coordinator to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities eg 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

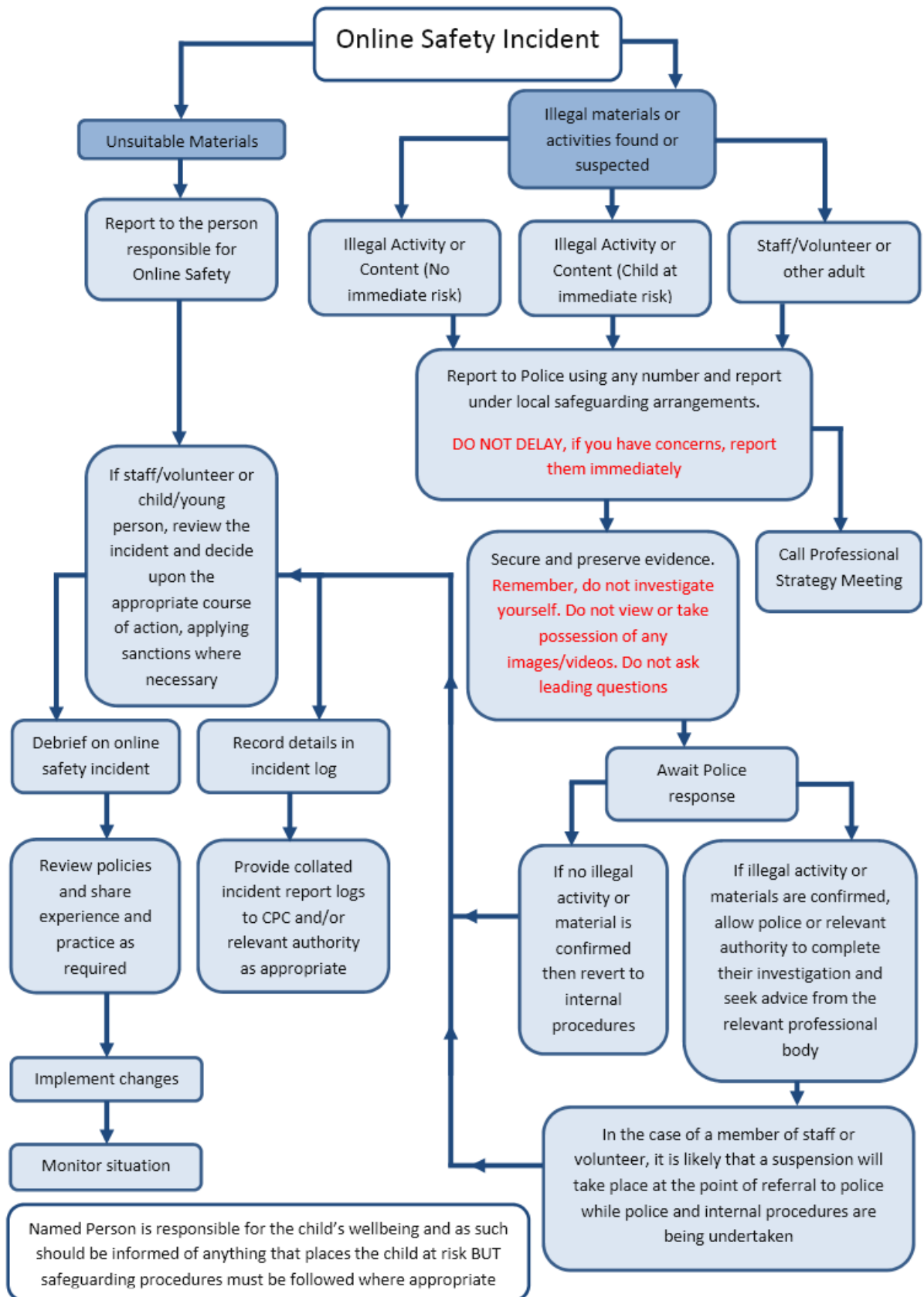
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse 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.



## 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

## Actions

Incidents:	Refer to class teacher / tutor	Refer to ICT Coordinator	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
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b>		X	X	X		X	X	X	
Unauthorised use of non-educational sites during lessons	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								
Attempting to access or accessing the school network, using another student's / pupil's account	X	X							
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X			X			
Corrupting or destroying the data of other users	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			
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			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	X						
Deliberately accessing or trying to access offensive or pornographic material	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
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b>		X	X	X				
Inappropriate personal use of the internet / social media / personal email	X	X	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 eg holding or transferring data in an insecure manner	X	X						
Deliberate actions to breach data protection or network security rules	X	X						
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X				X		
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X				X		
Actions which could compromise the staff member's professional standing	X	X				X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X		
Using proxy sites or other means to subvert the school's filtering system	X	X			X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X			
Deliberately accessing or trying to access offensive or pornographic material	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

Signed:

Date: Sept 25

Review: Sept 26

*O. Good*