recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital / video images to support educational aims, but must follow school procedures 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. Staff must not share / distribute any images unless consent has been given by parents and the leadership team.
- Care should be taken when taking digital / video images to ensure that the school is not led into disrepute.
- 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

Data Protection

Personal data is any information that, when combined with other information, could be used to identify an individual ("natural born person"). This brings a wide range of information within the scope of what is considered personal data.

This includes clear personal data, such as:

- Name
- Address
- Date of birth
- Email address
- Login details

But also data such as:

- Test scores (as this could be combined with other data to identify an individual)
- Car number plates

Extra precautions must be taken with special category data, such as:

- Medical or health information
- Race or ethnic origin
- Religion or politics

Data which could refer to a group of 5 or less is generally considered personal data.

Whenever personal data is collected, processed, stored, or destroyed, this must be in compliance with the General Data Protection Regulation (GDPR)

All personal data must be for a specific purpose, and have a lawful basis for processing, in line with the school's data policies.

All staff must ensure that they take the utmost care to protect personal data, and to ensure that pupils do the same.

Protection for this data includes:

- Only holding it in ways approved in the trust's data retention policy
- Following good security practice by always locking workstations, using a secure password
- Not transferring the data in insecure ways

In the event that any member of staff believes that personal data has, or might have been, handled or disclosed in a way outside of the data retention policy they MUST inform the data protection officer (Graham Newbery) immediately. Data breaches may have to be notified to the information commissioner within 72 hours of discovery, so time is of the essence.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies 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 / academy* or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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 /academy* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The *school's / academy's* use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

<u>Unsuitable / inappropriate activities</u>

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 certain internet 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					ü
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					ü
	adult material that potentially breaches the Obscene Publications Act in the UK					ü
	criminally racist material in UK					ü
	pornography				ü	
	promotion of any kind of discrimination				ü	
	promotion of racial or religious hatred				ü	
	threatening behaviour, including promotion of physical violence or mental harm				ü	
	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				ü	
Using school systems to run a private business					ü	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					ü	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					ü	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					ü	

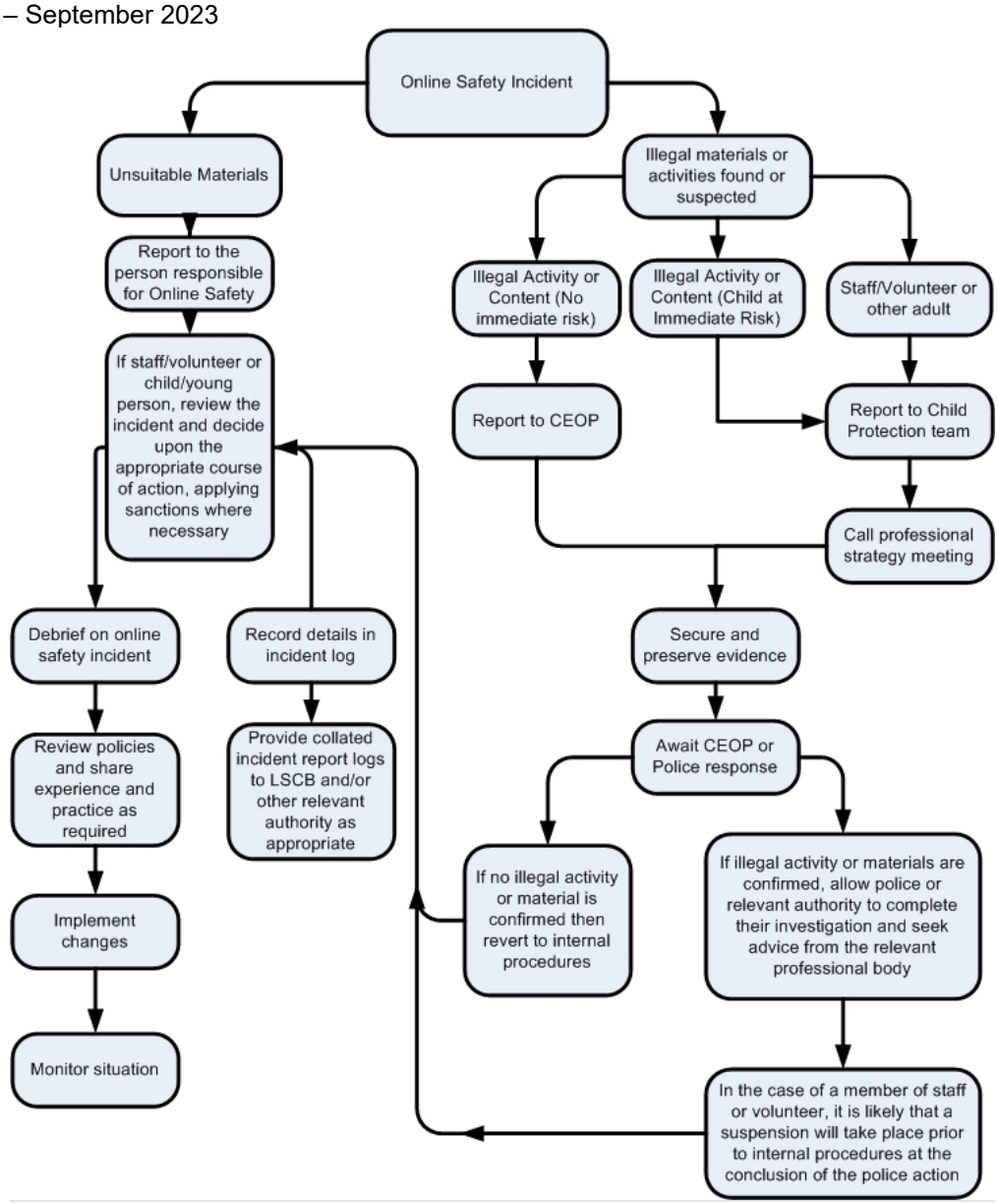
Creating or propagating computer viruses or other harmful files				ü	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				ü	
On-line gaming (educational)		ü			
On-line gaming (non educational)				ü	
On-line gambling				ü	
On-line shopping / commerce		ü			
File sharing				ü	
Use of social networking sites			ü		
Use of video broadcasting e.g. YouTube			ü		

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, i.e.:

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

refer to the right-hand side of the Flowchart for responding to online safety incidents and report immediately to the police.

The SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school / academy 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 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 / academy and possibly the police and demonstrate that visits to these sites were carried out for child protection 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:

Pupils	Actions								
Incidents:	Refer to class teacher / tutor	Refer to Leadership Team	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering /	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			ü	ü					
Unauthorised use of non-educational sites during lessons	ü								
Unauthorised use of mobile phone / digital camera / other handheld device	ü				ü				
Unauthorised use of social networking / instant messaging / personal email	ü								
Unauthorised downloading or uploading of files	ü								
Allowing others to access school network by sharing username and passwords		ü							
Attempting to access or accessing the school network, using another student's / pupil's account	ü								
Attempting to access or accessing the school network, using the account of a member of staff		ü	ü			ü			
Corrupting or destroying the data of other users	ü								
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		ü							
Continued infringements of the above, following previous warnings or sanctions		ü							

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		ü							
Using proxy sites or other means to subvert the school's filtering system		ü			ü				
Accidentally accessing offensive or pornographic material and failing to report the incident		ü	ü		ü	ü			
Deliberately accessing or trying to access offensive or pornographic material		ü	ü	ü			ü	ü	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		ü							

Staff **Actions**

Incidents:	Refer to Leadership t	Refer to ISP	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	ü	ü	ü	ü		ü
Inappropriate personal use of the internet / social networking sites / instant messaging / personal email	ü				ü	
Unauthorised downloading or uploading of files	ü					
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	ü				ü	

Careless use of personal data e.g. holding or transferring data in an insecure manner	ü					
Deliberate actions to breach data protection or network security rules	ü	ü				
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	ü	ü				ü
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	ü	ü				ü
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils not connected to education	ü			ü		ü
Actions which could compromise the staff member's professional standing	ü				ü	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	ü				ü	
Using proxy sites or other means to subvert the school's filtering system	ü					
Accidentally accessing offensive or pornographic material and failing to report the incident	ü			ü		
Deliberately accessing or trying to access offensive or pornographic material	ü					ü
Breaching copyright or licensing regulations	ü				ü	
Continued infringements of the above, following previous warnings or sanctions	ü					ü