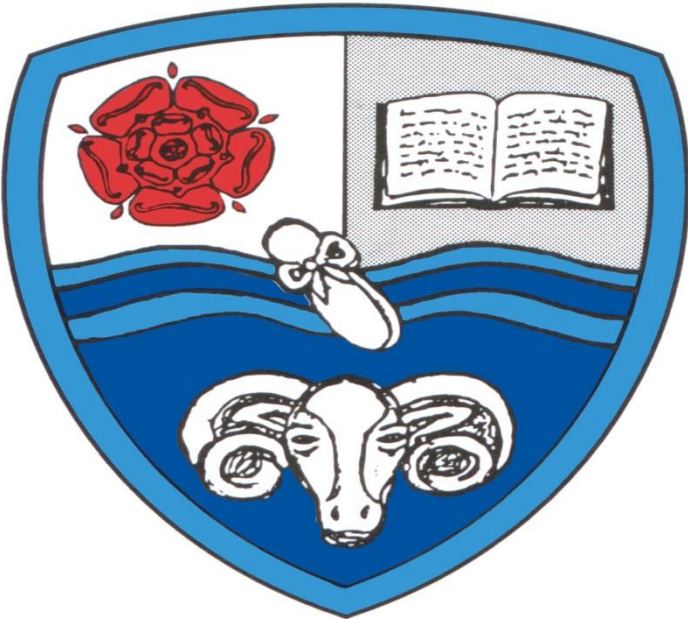# St Mary's CE Primary School

Online Safety Policy

SWGfL Online Safety School Template Policies

This policy applies to all governors, staff, pupils, parents and visitors to the school, including all contractors.

School Mission Statement
Based upon our belief of Jesus Christ as the Son of God and Saviour of the World, we will give all children a positive experience of Christianity and learning, whilst retaining a respect for other faiths.
We will promote the spiritual, moral, cultural, mental and physical development of all pupils, within a caring, loving, stimulating and nurturing environment, which is firmly based upon Christian values.
All children will receive a wealth of high quality educational experiences through the positive involvement of school, home and St. Mary's Church.

Development / Monitoring / Review of this Policy

This online safety policy has been developed in consultation with the whole school community has taken place through a range of formal and informal meetings.

- *Headteacher*
- *Staff – including Teachers and support staff*
- *Governors*
- *Parents and Carers*

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body*:*	
The implementation of this Online safety policy will be monitored by the:	*Headteacher and DSL – Mr N Gurman*
Monitoring will take place at regular intervals:	*At least annually*
The *Curriculum Committee* will receive a report on the implementation of the Online Safety policy generated by the monitoring group at regular intervals:	*At least annually*
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 e-safety or incidents that have taken place. The next anticipated review date will be:	September 2018
Should serious Online Safety incidents take place, the following external persons / agencies should be informed:	*: LA ICT Manager, LA Safeguarding Officer, Police*

The school will monitor the impact of the policy using:
- *Logs of reported incidents via CPOMS*
- *Monitoring logs of internet activity (including sites visited)*
- *Internal monitoring data for network activity*
- *Surveys / questionnaires of*
  - *students / pupils*
  - *parents / carers*
  - *staff*

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteacher's to such extent as is reasonable, to regulate the behaviour of pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of St Mary's CE Primary School. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that takes place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within St Mary's CE Primary School:

Governors / Board of Directors:

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 *Curriculum Committee* receiving regular information about Online safety incidents and monitoring reports. A member of the *Governing Body* has taken on the role of *Online Safety Governor*. The named Governor is Karen Girling. The role of the Online Safety *Governor* will include:

- *regular meetings with the Online Safety Co-ordinator – Mr Neil Gurman (DSL and Headteacher)*
- *regular monitoring of Online safety incident logs*
- *reporting to relevant Governors , meetings and committees*

Headteacher / Principal and Senior Leaders:

- *The Headteacher, Mr N Gurman has a duty of care for ensuring the safety (including Online safety) of members of the school community*.

- *The Headteacher and Mrs A Bedlow (Back-up DSL) 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 and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online safety monitoring role. 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 Co-ordinator, Mr N Gurman.*

South West Grid for Learning Trust Ltd, Belvedere House, Woodwater Park, Pynes Hill, Exeter EX2 5WS.

Tel. 0844 800 2382   **Email** esafety@swgfl.org.uk   **Website** www.swgfl.org.uk   © All rights reserved SWGfL 2013

3

Online Safety Coordinator / Officer:

The named Online Safety Co-ordinator for St Mary's CE Primary School is Mr N Gurman who is also the school's DSL.

Mrs A Bedlow is the school's back-up Online Safety Co-ordinator. The Online Safety Co-ordinator's role is to:

- reports to the curriculum 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 training and advice for staff
- liaises with the Local Authority / relevant body
- 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 the school's Online Safety *Governor, Mrs Girling* to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to Senior Leadership Team

All incidents will be recorded by any member of staff who has been involved and will then be passed onto the school DSL, Mr N Gurman. This will follow the same recording and reporting systems in place for safeguarding and Child Protection referrals via CPOMS.

Network Manager / Technical staff:

St Mary's CE Primary School has a managed ICT service provided by Mr J Kavanagh. It is the responsibility of the school to ensure that Mr Kavanagh carries out all the online safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that Mr Kavanagh is fully aware of St Mary's CE Primary School online safety policy and procedures.

The Network Manager / Technical Staff / Co-ordinator for ICT / Computing is responsible for ensuring:

- *that the school's technical infrastructure is secure and is not open to misuse or malicious attack*
- *that the school meets required online safety technical requirements and any Local Authority 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 network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction*
- *that monitoring software / systems are implemented and updated as agreed in school policies*

South West Grid for Learning Trust Ltd, Belvedere House, Woodwater Park, Pynes Hill, Exeter EX2 5WS.

Tel. 0844 800 2382   **Email** esafety@swgfl.org.uk   **Website** www.swgfl.org.uk   © All rights reserved SWGfL 2013

4

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)
- they report any suspected misuse or problem to the *Headteacher, Mr N Gurman or Mrs A Bedlow* for investigation / action / sanction
- all digital communications with 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
- pupils understand and follow the online safety and acceptable use 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

Child Protection / Safeguarding Designated Person / Officer

should be trained in online safety issues and be aware of the potential for serious child protection / 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

nb. it is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.

Pupils:

- are responsible for using the *school* digital technology systems in accordance with the Pupil *Acceptable Use Policy*
- 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 St Mary's CE Primary School Online Safety Policy covers their actions out of school, if related to their membership of the school

South West Grid for Learning Trust Ltd, Belvedere House, Woodwater Park, Pynes Hill, Exeter EX2 5WS.

Tel. 0844 800 2382   **Email** esafety@swgfl.org.uk   **Website** www.swgfl.org.uk   © All rights reserved SWGfL 2013

5

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. St Mary's CE Primary School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. 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

South West Grid for Learning Trust Ltd, Belvedere House, Woodwater Park, Pynes Hill, Exeter EX2 5WS.

Tel. 0844 800 2382   **Email** esafety@swgfl.org.uk   **Website** www.swgfl.org.uk   © All rights reserved SWGfL 2013

6

Policy Statements

Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be 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 Computing, PSHE and other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and class activities
- Pupils should be taught in all lessons to be critically aware of the materials / 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.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg 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 relevant designated 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 / carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line 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 / Carers sessions*
- *High profile events / campaigns e.g. Safer Internet Day*
- *A dedicated website page related to Online Safety for parents and pupils*

South West Grid for Learning Trust Ltd, Belvedere House, Woodwater Park, Pynes Hill, Exeter EX2 5WS.

Tel. 0844 800 2382   **Email** esafety@swgfl.org.uk   **Website** www.swgfl.org.uk   © All rights reserved SWGfL 2013

7

Education – The Wider Community

St Mary's CE Primary School will provide opportunities for the local 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 website will provide online safety information for the wider community

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.
- 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 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 meetings and INSET days.
- The Online Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors / Directors

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 / child protection. 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 (this may include attendance at assemblies / lessons).

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.

South West Grid for Learning Trust Ltd, Belvedere House, Woodwater Park, Pynes Hill, Exeter EX2 5WS.

Tel. 0844 800 2382   **Email** esafety@swgfl.org.uk   **Website** www.swgfl.org.uk   © All rights reserved SWGfL 2013

8

- All users in KS2, KS1, EYFS will be provided with class log-ons and staff are made aware of the associated risks which are described in the appendix.
- **The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the *Headteacher* and kept in a secure place.**
- The ICT Co-ordinator is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- **Internet access is filtered for all users by BT Lancashire Services.** Illegal content 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. There is a clear process in place to deal with requests for filtering changes.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed. This is the same procedure as Child Protection and Safeguarding issues.
- 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 for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems. Guests will use the general staff member log in.
- *An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.*
- *An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.*
- *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.* Staff are only allowed to use the removable, encrypted USB memory stick provided by school in school, for school data/information. No other USB's are allowed in school or for saving work related information on.

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 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, 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 in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other 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 pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission

South West Grid for Learning Trust Ltd, Belvedere House, Woodwater Park, Pynes Hill, Exeter EX2 5WS.

Tel. 0844 800 2382   **Email** esafety@swgfl.org.uk   **Website** www.swgfl.org.uk   © All rights reserved SWGfL 2013

9

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- 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 pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR school policies 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". (see Privacy Notice section in the appendix)
- It has a Data Protection Policy.
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- 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 provided by the school.**

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

South West Grid for Learning Trust Ltd, Belvedere House, Woodwater Park, Pynes Hill, Exeter EX2 5WS.

Tel. 0844 800 2382   **Email** esafety@swgfl.org.uk   **Website** www.swgfl.org.uk   © All rights reserved SWGfL 2013

10

SWGfL Online Safety School Template Policies

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				Pupils			
	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							x
Use of mobile phones in lessons		X						X
Use of mobile phones in social time	X							X
Taking photos on personal 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	

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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.
- 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 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 email addresses may be used at KS1, while pupils at KS2 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

Please refer to the Use of Social Media Policy the Governors adopted from LCC.

Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist/ terrorist related 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,	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

South West Grid for Learning Trust Ltd, Belvedere House, Woodwater Park, Pynes Hill, Exeter EX2 5WS.

Tel. 0844 800 2382   **Email** esafety@swgfl.org.uk   **Website** www.swgfl.org.uk   © All rights reserved SWGfL 2013

12

remarks, proposals or comments that contain or relate to:	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 / academy					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				

South West Grid for Learning Trust Ltd, Belvedere House, Woodwater Park, Pynes Hill, Exeter EX2 5WS.

Tel. 0844 800 2382   **Email** esafety@swgfl.org.uk   **Website** www.swgfl.org.uk   © All rights reserved SWGfL 2013

13

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.
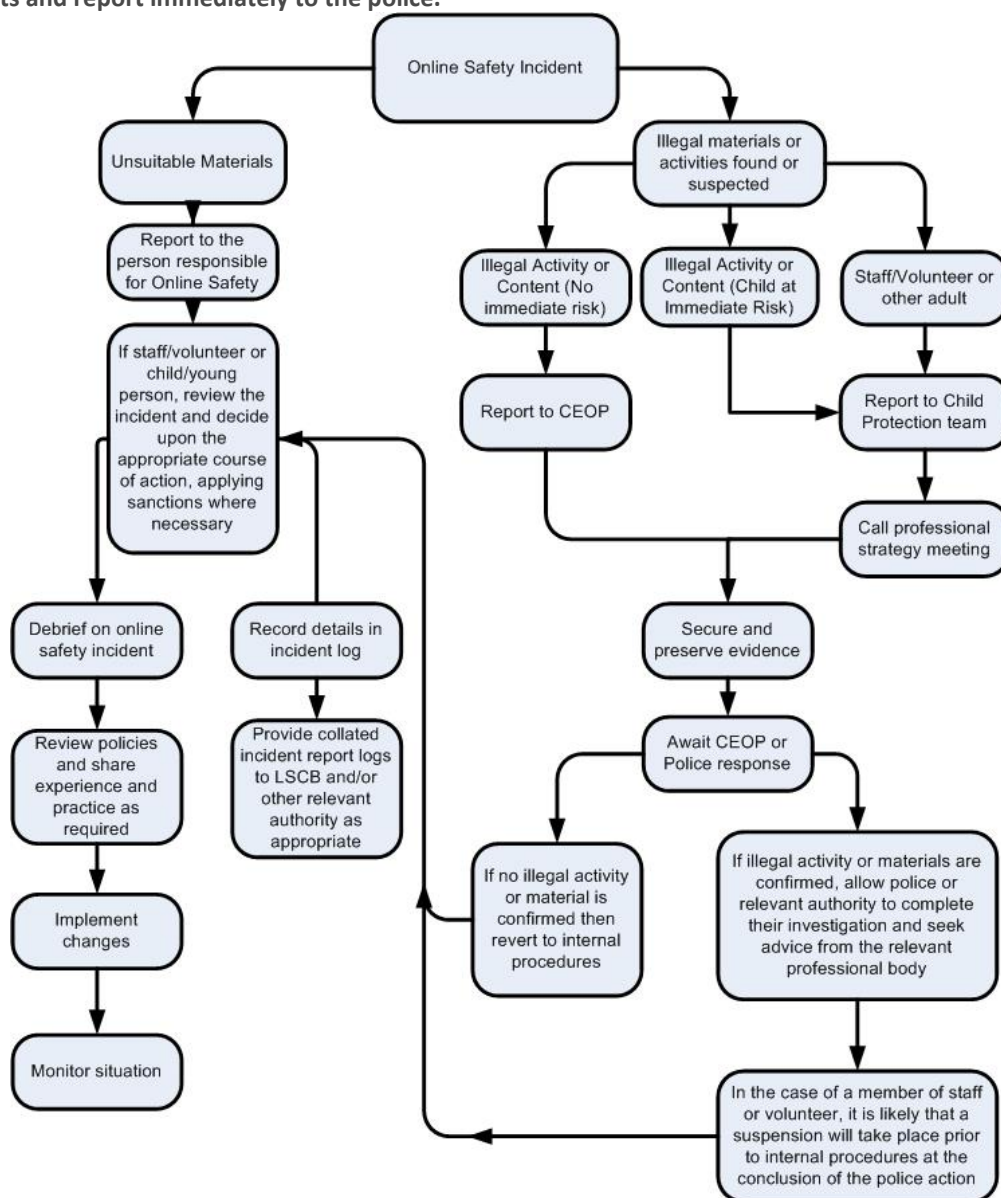
Other Incidents

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 child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

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:

Actions / Sanctions

South West Grid for Learning Trust Ltd, Belvedere House, Woodwater Park, Pynes Hill, Exeter EX2 5WS.

Tel. 0844 800 2382   **Email** esafety@swgfl.org.uk   **Website** www.swgfl.org.uk   © All rights reserved SWGfL 2013

15

Students / Pupils

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	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	X	X	X		X
Unauthorised use of non-educational sites during lessons	X		X			X		X	
Unauthorised use of mobile phone / digital camera / other mobile device	X		X			X		X	X
Unauthorised use of social media / messaging apps / personal email	X		x			X		X	X
Unauthorised downloading or uploading of files	X		X			X		X	X
Allowing others to access school / academy network by sharing username and passwords			X			x	x	X	
Attempting to access or accessing the school / academy network, using another student's / pupil's account	X		X					X	
Attempting to access or accessing the school / academy network, using the account of a member of staff	x		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	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	X
Using proxy sites or other means to subvert the school's / academy'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		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X		X	X	X	X	X

Staff   Actions / Sanctions

Incidents:	Refer to line managerr	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			X
Inappropriate personal use of the internet / social media / personal email	X	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		x
Careless use of personal data eg holding or transferring data in an insecure manner	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
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 / academy into disrepute or breach the integrity of the ethos of the school / academy	X	X				X		
Using proxy sites or other means to subvert the school's / academy's filtering system	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
Breaching copyright or licensing regulations	X	X				X		X
Continued infringements of the above, following previous warnings or sanctions	X	X					X	X

South West Grid for Learning Trust Ltd, Belvedere House, Woodwater Park, Pynes Hill, Exeter EX2 5WS.

Tel. 0844 800 2382   **Email** esafety@swgfl.org.uk   **Website** www.swgfl.org.uk   © All rights reserved SWGfL 2013

18