Somerford Primary School

Online Safety Policy

Introduction

New technologies have become integral to the lives of children and all staff in today's society, both within schools and in their lives outside school.   The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and all staff learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and all staff should have an entitlement to safe internet access at all times.

The requirement to ensure that children and all staff are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school online safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, carers, members of the community and the all staff themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.   However, the use of these new technologies can put all staff at risk within and outside the school. Some of the dangers they may face include:

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

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).
As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build all staff' resilience to the risks to

which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The online safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help all staff (and our parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Aims

The Online Safety Policy aims to outline safe and effective practice in the use of the internet. It provides advice on acceptable use and effective measures to enable children, all staff and adults to use computing resources in a safer online environment.

Development of this Policy

This online safety policy has been developed by the online safety committee made up of:
* *School Online Safety Champion*
* *Head of School*
* *Snr. Admin Officer*
* *Support Staff*
* *Computing Technical staff*
* *Governors and teachers*

Consultation with the whole school community has taken place through the following:
* *Staff meetings*
* *INSET Day*
* *Governors meeting*
* *School website / newsletters/student home school book*

Schedule for Development / Monitoring / Review

This online safety policy will be approved by the *Governing Body on:*	*Autumn 2019*
The implementation of this online safety policy will be monitored by the: online safety committee	(see above)
Monitoring will take place annually	Annually
The *Governing Body* will receive an report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) annually	*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 online safety or incidents that have taken place. The next anticipated review date will be:	*September 2020*
Should serious online safety incidents take place, the following external persons / agencies should be informed as appropriate	*LA Computing Manager, LA Safeguarding Officer, Police Commissioner's Office*

The school will monitor the impact of the policy using:
- *Logs of reported incidents*
- *SWGfL monitoring logs of internet activity (including sites visited)*
- *Staff pro-actively monitoring social media websites for public postings about the school and its staff*
- *Surveys / questionnaires of*
  - ∗ *students / all staff (eg Ofsted "Tell-us" survey / CEOP ThinkUknow survey)*
  - ∗ *parents / carers*
  - ∗ *staff*

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of all staff 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 out of school, but is linked to membership of the school. 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 take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety 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 *Governors* receiving regular information about online safety incidents and monitoring reports. The Governing Body has nominated an *Online Safety Governor (Ken Stevenson)*. The role of the Online Safety Governor will include:
- *regular meetings with the Online safety Champions*
- *regular monitoring of online safety incident logs*
- *regular monitoring of filtering / change control logs*
- *reporting to relevant Governors committee / meeting*

Headteacher and Senior Leaders:

- **The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community**, though the day to day responsibility for online safety will be delegated to the *Online safety Champion*.
- *The Headteacher / Senior Leaders are responsible for ensuring that the Online safety Champion and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant*
- *The Headteacher / 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 / Senior Management Team will receive regular monitoring reports from the Online safety Champion.*
- **The Headteacher and another member of the Senior Leadership 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.** (see SWGfL flow chart on dealing with online

safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures)

Online Safety Champion:
Michelle Semple is the school's designated Online Safety Champion who has the day to day responsibility for online safety who :
- 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 training and advice for staff
- liaises with the Local Authority
- liaises with school computing technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments, (Examples of suitable log sheets may be found in the SWGfL Safety and Security Booklet, along with the Internet Safety Protocol)
- meets regularly with Online safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team
  (The school will need to decide how these incidents will be dealt with and whether the investigation / action / sanctions will be the responsibility of the Headteacher.

Network Manager / Technical staff:
The school has a managed computing service provided by an outside contractor (Turn It On) whose responsibility is to ensure that the online safety measures that would otherwise be the responsibility of the school's technical staff, as suggested below, are implemented. It is also important that the managed service provider is fully aware of the SWGfL Security Policy and Acceptable Usage Policy.)
The Online Safety Committee is responsible for ensuring:
- that the school's computing infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- SWGfL is informed of issues relating to the filtering applied by the Grid
- the school's filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keeps 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* is regularly monitored in order that any misuse /attempted misuse can be reported to the *Headteacher.*

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 school Staff Acceptable Use Policy / Agreement (AUP)

- they report any suspected misuse or problem to the Online Safety Officer/Headteacher.
- online safety issues are embedded in all aspects of the curriculum and other school activities
- All staff understand and follow the school online safety and acceptable use policy
- they monitor computing activity in lessons, extra curricular and extended school activities
- they are aware of online safety issues related to the use of mobile phones, games consoles, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned all staff 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

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

Online safety Committee
Members of the *Online safety committee* will assist the *Online safety Champion* with:
- the production / review / monitoring of the school online safety policy / documents.
- *the production / review / monitoring of the school filtering policy*

Students / all staff:
- **are responsible for using the school computing systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.** (at KS1 it would be expected that parents / carers would sign with all staff. A copy is in the home school book.)
- 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school 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 / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of computing than their children. The school will therefore 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 responsible for:
- endorsing (by signature) the Pupil Acceptable Use Policy

Policy Statements

Education – students / all staff

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

Online safety education will be provided in the following ways:

- A planned online safety programme should be provided as part of computing and PHSE and should be regularly revisited – this will cover both the use of computing and new technologies in school and outside school
- Key online safety messages should be reinforced as part of a planned programme of assemblies.
- all staff 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
- all staff should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of computing, the internet and mobile devices both within and outside school
- Rules for use of computing systems / internet will be posted in all rooms and displayed on log-on screens
- Staff should act as good role models in their use of computing, the internet and mobile devices

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 experiences. Parents often either underestimate or do not realise how often children and all staff come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

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

- *Letters, newsletters,*
- *Web site*
- *Face-to-face meetings*

Education & Training – Staff

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.
- 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 Policies
- *The Online safety Coordinator will receive regular updates through attendance at SWGfL / LA / other information / training sessions and by reviewing guidance documents released by BECTA / SWGfL / LA and others.*
- *This Online safety policy and its updates will be presented to and discussed by staff in staff / team meetings.*
- *The Online safety Coordinator will provide advice / guidance / training as required 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 computing / 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 / SWGfL or other relevant organisation.
• Participation in school training / information sessions for staff or parents

Technical – infrastructure , equipment, filtering/monitoring/password security

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 computing systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online safety Policy and guidance
• There will be regular reviews and audits of the safety and security of school computing systems
• Servers, wireless systems and cabling must be securely located and physical access restricted
• All users will have clearly defined access rights to school computing systems. Details of the access rights available to groups of users will be recorded by the Network Manager June Hill and will be reviewed, at least annually, by the Online safety Committee
• All users (at KS2 and above) will be provided with a username and password by Snr. *Admin officer June Hill who will keep an up to date record of users and their usernames. Users will be required to change their password every term.*
• The "master / administrator" passwords for the school computing system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school safe)
• *Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.*
• *The school maintains and supports the managed filtering service provided by SWGfL*
• *In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).*
• *Any filtering issues should be reported immediately to SWGfL.*
• *Requests from staff for sites to be removed from the filtered list will be considered by the Admin Officer and Headteacher. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online safety Committee*
• *School computing technical staff regularly monitor and record the activity of users on the school computing systems and users are made aware of this in the Acceptable Use Policy.*
• *An appropriate system is in place for users to report any actual / potential online safety incident to the Senior Admin Officer, June Hill or Headteacher. An Online safety concern form will need to be completed.*
• *Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.*

- *An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system.*
- *An agreed policy is in place regarding the downloading of executable files by users*
- *An agreed policy is in place regarding the extent of personal use that users (staff / students / all staff / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.*
- *An agreement is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices.*
- *The school infrastructure and individual workstations are protected by up to date virus software.*
- *Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.*

Curriculum
Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of COMPUTING across the curriculum.

- *in lessons where internet use is pre-planned, it is best practice that all staff 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 all staff are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the all staff visit.*
- *It is accepted that from time to time, for good educational reasons, students 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 Network Manager (and other relevant 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.*

Use of digital and video images - Photographic, Video
The development of digital imaging technologies has created significant benefits to learning, allowing staff and all staff instant use of images that they have recorded themselves or downloaded from the internet. However, staff and all staff need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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 all staff 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.
- *Staff 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 all staff are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*
- All staff must not take, use, share, publish or distribute images of others without their permission
- *Photographs published on the website, or Marvellous Me that include all staff will be selected carefully and will comply with good practice guidance on the use of such images.*

- *All staff' 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 all staff 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 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.

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, USB stick or any other removable media:

- the data must be encrypted.
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software and regularly updated.
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

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

Communication Technologies	Staff & other adults				Students / All staff			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed but stored in school reception during school hours	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 mobile phones or other camera devices				X				X
Use of hand held devices eg PDAs, PSPs	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 chat rooms / facilities				X				X
Use of instant messaging				X				X
Use of social networking sites				X				X
Use of blogs (Twitter, Marvellous Me)	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.** *Staff should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).*
- **Users need to be aware that email communications may be monitored**
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email. They are to complete the online safety concern form.**
- **Any digital communication between staff and all staff or parents / carers (email, etc) must be professional in tone and content.**

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

User Actions

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:		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	child sexual abuse images					X
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					X
	adult material that potentially breaches the Obscene Publications Act in the UK					X
	criminally racist material in UK					X
	pornography				X	
	promotion of any kind of discrimination				X	
	promotion of racial or religious hatred				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	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					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	
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					X	
On-line gaming (educational)		X	X			
On-line gaming (non educational)			X			
On-line gambling				X	X	
On-line shopping / commerce			X		X	
File sharing					X	
Use of social networking sites			X		X	
Use of video broadcasting eg Youtube		X			X	

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of computing, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

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

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.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

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 and in accordance with other school policies

Students / All staff   Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to phase leader	Refer to Headteacher/Deputy	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights (fixed term)	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).		1	2						
Unauthorised use of non-educational sites during lessons	1				2		4	3	
Unauthorised use of mobile phone / digital camera / other handheld device	1	2							
Unauthorised use of social networking / instant messaging / personal email	1				2		4	3	
Allowing others to access school network by sharing username and passwords	1				2			3	
Attempting to access or accessing the school network, using another student's / pupil's account	1				2		4	3	
Attempting to access or accessing the school network, using the account of a member of staff			1		2		3		
Corrupting or destroying the data of other users			1		2		3		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature			1	3		2	5		4
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			1			2	3		
Using proxy sites or other means to subvert the school's filtering system			1	5	2	3	4		
Accidentally accessing offensive or pornographic material and failing to report the incident	1							2	
Deliberately accessing or trying to access offensive or pornographic material		1	3		2				

Staff   Actions / Sanctions

** Severity of Sanctions 1 – 5 with 1 being least serious.

Incidents:	Refer to line manager	Refer to Headteacher	RRefer 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).		1	2	3			4	
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	1	2						
Unauthorised downloading or uploading of files	1	2						
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		1			2			
Careless use of personal data eg holding or transferring data in an insecure manner	1	2						
Deliberate actions to breach data protection or network security rules		1				2		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		1		3	2	4		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		1		2			3	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / all staff		1	3					
Actions which could compromise the staff member's professional standing		1				2		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		1	2					
Using proxy sites or other means to subvert the school's filtering system		1		3	2			
Accidentally accessing offensive or pornographic material and failing to report the incident		1			2			
Deliberately accessing or trying to access offensive or pornographic material		1	3	4			2	
Breaching copyright or licensing regulations		1						

Personal use **of parents/carers**

If parents/carers choose to use social media to post comments relating to the school, they are encouraged to use appropriate comments. In any event where the reputation of the school and its staff are called into question (posting inappropriate or offensive comments), then the school will ask the parents/carers to remove these posts and invite them to discuss the issues in person. If necessary, parents can be referred to the school's complaints procedures.

Acknowledgements

- Swindon Borough Council
- Poole Borough Council
- Bournemouth Borough Council
- North Somerset Council
- Gloucestershire County Council
- DCSF
- Becta
- National Education Network (NEN)
- London Grid for Learning
- Kent County Council
- Northern Grid for Learning
- Bracknell Forest Borough Council
- Byron Review – Children and New Technology – "Safer Children in a Digital World"

SIGNED : ……………………………………..   DATE : …………………………………
      Online Safety Champion

SIGNED : ……………………………………….   DATE : …………………………………….
      Headteacher

SIGNED : ……………………………………..   DATE : …………………………………….
      Chair of Governors