Sunninghill
PREP SCHOOL DORCHESTER

E-Safety Policy

Incorporating: bring your own device, communications and technical Infrastructure

May 2017

360safe
the e-safety self review tool

SOUTH WEST
GRID
FOR LEARNING

Rationale

New technologies have become integral to the lives of children and young people 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 pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people 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. The development and implementation of such a strategy involves all the stakeholders in a child's education from the head teacher and governors to the SLT and classroom teachers, support staff, parents, members of the community and the pupils 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 young people at risk within and outside the school.

Some of the dangers children 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 E-Safety Policy is used in conjunction with other school policies (e.g. mobile phone use, behaviour, acceptable use, anti-bullying and safeguarding policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' 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.

Monitoring and Review of this Policy

This E-Safety Policy has been developed by a working group made up of:

- School E-Safety Coordinator (Head of Computing)
- Deputy Head in charge of pastoral care
- ICT Technical support (Flatrock Systems Ltd)
- Safeguarding Governor

Child views have been taken into consideration via class discussions in e-safety lessons.

Schedule for Development / Monitoring / Review

The implementation of this E-Safety Policy will be monitored by the:	Head of Computing and the Head
Monitoring will take place at regular intervals:	Annually
The E-Safety Policy will be reviewed annually or more regularly in the light of any significant new developments in the use of the technologies or new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	January 2016
Should serious e-safety incidents take place, the following external persons/ agencies should be informed:	Safe Schools team, Dorset Police (SSCT) Tel: 01202 222844 E-mail: ssct@dorset.pnn.police.uk Web: http://www.stopthinkdorset.co.uk/ Safeguarding Officer for Dorset CC

The school will monitor the impact of the policy using:

- Logs of reported incidents
- South West Grid for Learning(SWGfL) monitoring logs of internet Internal monitoring data for network activity
- Feedback from teaching and learning support staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Heads 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 e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see our new Electronic Devices-Searching and Deletion policy which is currently in a draft form). 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/guardians of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of E-Safety Governor - **Mr R. Miller (chairman).**

The role of the E-Safety Governor will include:

- regular meetings with the Child Protection officer and E-Safety Co-ordinator to discuss any e-safety incident log entries, filtering issues etc.
- reporting to the Board of Governors as required

Head teacher and Senior Leaders:

- The Head has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator (Head of Computing).
- The Head and Deputy Head (Pastoral) should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents "Responding to incidents of misuse" in Appendix.
- The Head / Senior Leadership Team (SLT) are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues.
- To ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role, all issues will be brought to the attention of the Deputy Head (Pastoral).
- The Senior Leadership Team will receive monitoring updates from the E-Safety Co-ordinator.

E-Safety Co-ordinator (Head of Computing):

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-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 e-safety incidents and creates a log of incidents to inform future e-safety developments (stored on the Staff drive: ICT/E-safety incidents reporting log.doc)
- meets with the Deputy Head (Pastoral) and / or E-Safety Governor to discuss any current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors, as requested
- reports regularly to the Deputy Head (Pastoral)
- liaises with the Deputy Head (Pastoral) or Head to decide how e-safety incidents will be dealt with and whether the investigation / action / sanctions needed

Network Manager/Technical staff:

Network support is provided by Flatrock Systems Ltd 01305 262306. The Network Manager and Head of Computing are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and guidance
- that sub-contracted IT support companies or shared technicians are aware of school policy on e-safety
- that users may only access the school's networks through their password protected account, 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 keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network/ remote access/e-mail may be regularly monitored in order that any misuse/attempted misuse can be reported to the E-Safety Co-ordinator or Head for investigation / action / sanction
- The establishment may exercise its right by electronic means to monitor the use of the computer systems, including: the monitoring of websites, the interception of emails and the deletion of inappropriate materials, in circumstances where it believes unauthorised or inappropriate use of the establishment's computer system is or may be taking place, or the system is or may be being used for criminal purposes, or for storing text or imagery which is unauthorised or unlawful.
- Inspections will be made in response to complaints.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and have read the current school E-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 E-Safety Co-ordinator, SLT or Head for appropriate investigation/action/sanction
- all digital communications with pupils (e-mail/voice) must be on a professional level and carried out using official school systems where at all possible.
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, 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, 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
- Staff may request a login to the staff proxy to bypass the filter. **Great care must be taken in its use and 'Safe search settings' should be manually enabled where needed e.g. Google and Youtube.**

Child Protection / Safeguarding Designated Person

The Deputy Head (Pastoral) should be trained in e-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

Pupils:

- Forms 3 – 8 are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy (AUP). They will be expected to sign the AUP before being given access to school systems (parents/guardians can sign on behalf of the younger pupils).
- new pupils sign a copy of the AUP on entry to the school. Pupils are reminded of the contents of the policy annually and sign a pre-printed page in their school diaries.
- 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 e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents/guardians

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, Hermes newsletters, letters, school website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / and on-line pupil records (3sys)
- their children's personal devices in the school (where this has been allowed)

Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy on entry to the school
- accessing the school website/parent portal (3sys) in accordance with the relevant school Acceptable Use Policy.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. E-safety should therefore be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education is provided in the following ways:

- A planned e-safety programme is provided as part of Computing. The school scheme of work is updated annually to include best practise but based on the scheme from SWGfL http://www.digital-literacy.org.uk/Home.aspx
- Key e-safety messages are reinforced in assemblies where appropriate e.g. anti-bullying
- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the Pupil AUP 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. 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, students may need to research topics (eg racism, drugs and discrimination) that would normally result in internet searches being blocked. Staff can request that the Head of Computing can temporarily remove those sites from the filtered list for the period of study.

Education – parents/guardians

Many parents and carers have only a limited understanding of e-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:

- Letters, Hermes school newsletters
- The school website e-safety page www.sunninghillprep.co.uk
- Parents evenings and specific e-safety information evenings (given annually)
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications eg www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers (see appendix for further links / resources)

Education & Training – Staff

- All staff should receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements (signed agreement to be filed in staff records).

- The E-Safety Coordinator will receive regular updates through attendance at external training events (eg from SWGfL / other relevant organisations), by signing up for regular email updates and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings or during Inset days.
- The E-Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors

Governors will take part in e-safety training / awareness session,

- either by completing an on-line course
- or participation in school training / information sessions for staff, parents or governors

Technical – infrastructure/equipment, filtering and monitoring

1. There will be annual reviews of the safety and security of school technical systems in school
2. Where possible, servers, wireless systems and cabling should be securely located and physical access restricted
3. All users will have clearly defined access rights to school technical systems and devices
4. All users (at KS2 and above) will be provided with a username and password by the Head of Computing. Users are responsible for the security of their username and password and will be reminded to change their password termly
5. The "administrator" passwords for the school ICT systems, used by the Network Manager must also be available to Bursar
6. Flatrock Systems 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
7. Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the SWGfL filtering service. Content lists are regularly updated. Requests for filtering changes are to be made to the Head of Computing.
8. The school technical staff may monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
9. Any actual / potential technical incident / security breach should be reported to the Head of Computing.
10. Appropriate security measures (passwords) 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. The school infrastructure and individual workstations are protected by up to date virus software.
11. Guest logins are not allowed. All users will need to request a login from the Head of Computing and sign an AUP before access will be granted.
12. Only administrator logins allow the downloading of executable files and installation of programmes on school devices.
13. The school recommends that personal data concerning staff or pupils is not sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Memory sticks / external hard drives without security measures are not a safe method to transfer sensitive data.

Bring Your Own Device (BYOD) - Staff, Pupils and Visitors

See separate school staff Mobile Phone Policies – Main School and Early Years

Pupils are not currently permitted to bring devices into school unless there is a recognised educational or physical need e.g. use of a word processor in English for a child with dyslexia. Permission should be sought from the Head. Devices are brought into school at the risk of the owner. Staff may bring in personal devices but at their own risk.

- All users may access their devices in accordance with the school Acceptable Use Agreement
- The device must include up-to-date virus and malware checking software
- All network systems are secure and access for users is differentiated
- Where possible, these devices will be covered by the school's normal filtering systems, while being used on the premises (excludes 3G, 4G)
- Any device loss, theft, change of ownership of the device is to be reported to the Bursar or Head of Computing.
- Any user leaving the school will follow the processes outlined within the Confirmation of end of contract letter including the removal of all school data
- The school adheres to the Data Protection Act principles

Use of digital and video images – Staff and Pupils

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 cyber-bullying to take place. The school aims 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 e.g. on social networking sites.
- Parents are advised not to take images / videos without permission. To respect everyone's privacy and in some cases protection, images should not be published on social networking sites, nor should parents / carers comment on any activities involving other pupils.
- 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. It is recommended that 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
- Photographs or videos 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 sought on entry to the school. Only images of pupils whose parents have given their permission may be used for marketing purposes or published on the school website.

Data Protection Refer to the school Data Protection Policy

When personal data is stored on any portable computer system, memory stick, or any other removable media or device (including phones), the school strongly recommends that staff:

- 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
- ensure that they are properly "logged-off" at the end of any session or 'remote' session
- transfer data using encryption and secure password protected devices where possible
- access sensitive / personal data from home using their 'remote' login rather than copying data onto unprotected memory sticks or external hard drives
- securely delete data from any device once it has been transferred or its use is complete
- report any loss or theft of a removable / portable device containing sensitive / personal data to the Bursar or Head of Computing as soon as possible.

Communications - Staff and Pupils

The following table shows how the school currently considers the benefit of using these technologies for education balances against their risks / disadvantages:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not recommended	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought school	✓						✓	
Use of mobile phones in lessons			✓					✓
Use of mobile phones in social time		✓					✓	
Taking photos on school mobile phones or other school camera devices (excludes EYFS)	✓						✓	
Taking photos / videos on personal devices				✓				✓
Use of other mobile devices eg tablets, gaming devices		✓					✓	
Use of personal e-mail addresses in school, or on school network		✓					✓	
Use of school e-mail for personal e-mails		✓					✓	
Use of instant messaging		✓					✓	
Use of social networking sites		✓					✓	
Use of blogs	✓						✓	

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

- The official school e-mail service may be regarded as safe and secure. It is strongly recommended that staff and pupils should use only the school e-mail service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that e-mail communications may be monitored
- Users must immediately report, the receipt of any e-mail that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such e-mail.
- Any digital communication between staff and pupils or parents/guardians (e-mail, chat) must be professional in tone and content. These communications should only take place on official school systems.
- Personal information should not be posted on the school website and only official e-mail addresses should be used to identify members of staff.

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 usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					✓
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					✓
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					✓
	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					✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	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				✓	
Using school systems to run a private business					✓	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					✓	
Infringing copyright					✓	

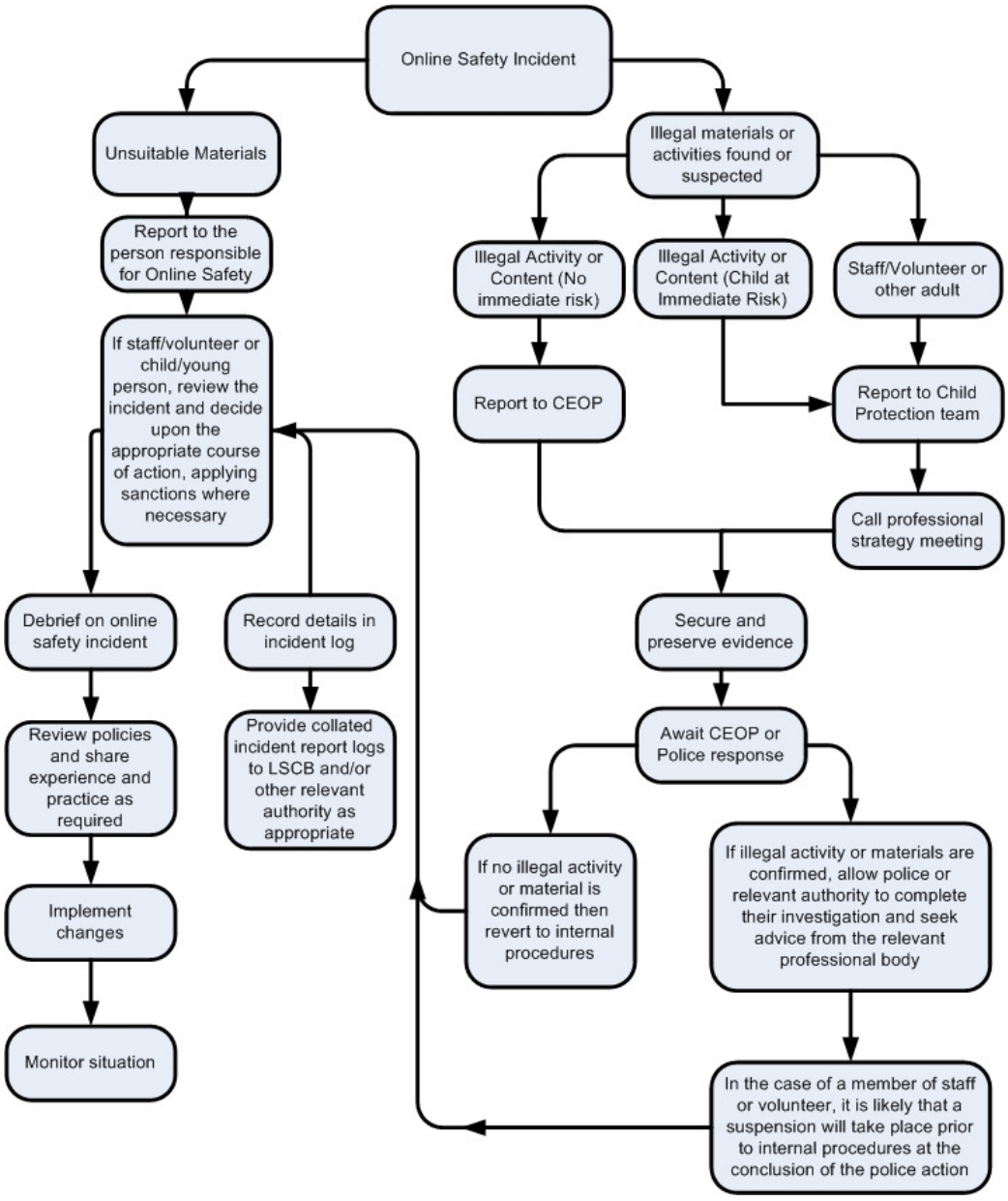
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				✓	
Creating or propagating computer viruses or other harmful files				✓	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				✓	
On-line gaming (educational)		✓			
On-line gaming (non educational)		✓			
On-line gambling				✓	
On-line shopping / commerce		✓			
File sharing	✓				
Use of social media		✓			
Use of messaging apps		✓			
Use of video broadcasting eg Youtube	✓				

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 for responding to online safety incidents and report immediately to the police.
http://www.swgfl.org.uk/products-services/Online-Safety-Services/E-Safety-Resources/creating-an-esafety-policy



Other Incidents

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:

Students / Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Com puting or Deputy Head (Pastoral)	Refer to Head	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).		✓	✓	✓					
Unauthorised use of non-educational sites during lessons	✓								
Unauthorised use of mobile phone / digital camera / other mobile device	✓	✓							
Unauthorised use of social media / messaging apps / personal email	✓	✓							
Unauthorised downloading or uploading of files		✓			✓				
Allowing others to access school network by sharing username and passwords	✓	✓							
Attempting to access or accessing the school network, using another student's / pupil's account		✓							
Attempting to access or accessing the school network, using the account of a member of staff		✓	✓		✓				
Corrupting or destroying the data of other users		✓			✓				
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		✓				✓			
Continued infringements of the above, following previous warnings or sanctions		✓	✓				✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓	✓						
Using proxy sites or other means to subvert the school's / academy's filtering system		✓			✓		✓		
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓			✓				
Deliberately accessing or trying to access offensive or pornographic material		✓	✓		✓	✓	✓		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓							

Staff Actions / Sanctions

Incidents:	Refer to line manager/ Head of Computing	Refer to Head teacher	Refer to bursar	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).		✓	✓	✓		✓	✓	✓
Inappropriate personal use of the internet / social media / personal email		✓				✓	✓	✓
Unauthorised downloading or uploading of files	✓	✓						
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	✓					✓		
Careless use of personal data eg holding or transferring data in an insecure manner	✓		✓			✓		
Deliberate actions to breach data protection or network security rules		✓	✓			✓		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓	✓			✓		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		✓	✓					✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		✓	✓			✓		
Actions which could compromise the staff member's professional standing		✓				✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓						✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓				✓	✓		
Deliberately accessing or trying to access offensive or pornographic material		✓						✓
Breaching copyright or licensing regulations			✓			✓		
Continued infringements of the above, following previous warnings or sanctions		✓						✓

Useful Links:

Safe Schools Team
Email: ssct@dorset.pnn.police.uk
Tel: 01202 222844

Useful E-safety Resources:

General

- Resource list provided by SWGfL: http://www.swgfl.org.uk/products-services/Online-Safety-Services/E-Safety-Resources/E-Safety-Resources
- SWGfL http://www.swgfl.org.uk/Staying-Safe
- The Dorset Police SSCT (Safe School and Communities Team) publish useful e-safety newsletters available here: Stop Think Dorset parents e-safety newsletters.
- Parenting in the Digital Age (or PitDA for short): Parenting in the Digital Age Website
- Ofcom's guidelines on safe use of the internet: Ofcom
- DASP E-Safety Web Page http://www.dasp.org.uk/e-safety.htm
- Child Exploitation and Online Protection Centre http://www.ceop.gov.uk/
- Thinkuknow http://www.thinkuknow.co.uk/
- Childnet International http://www.childnet.com
- Safer Internet Day http://www.saferinternet.org/ww/en/pub/insafe/index.htm
- Get Safe Online http://www.getsafeonline.org
- Cyberbullying.org - http://www.cyberbullying.org/

Social Networking

Digizen – Social Networking

SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people

Connect safely Parents Guide to Facebook

Facebook Guide for Educators

Curriculum

SWGfL Digital Literacy & Citizenship curriculum

Professional Standards / Staff Training

DfE - Safer Working Practice for Adults who Work with Children and Young People

Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs

Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs

UK Safer Internet Centre Professionals Online Safety Helpline

Policy

SWGfL http://www.swgfl.org.uk/Staying-Safe/Creating-an-E-Safety-policy

SWGfL 360 audit tool http://www.swgfl.org.uk/search-2.aspx?searchtext=360&searchmode=anyword