Freshford Church of England Primary School
E-Safety Policy

The e-Safety Policy will be part of the School Development Plan and relates to other policies including those for data protection, password security, mobile phone and camera use, the acceptable use of the Internet, anti-bullying, and for Child Protection.

Development/Monitoring of this policy

This e-safety policy has been developed by the Safeguarding Committee made up of:

- Headteacher / Principal / Senior Leaders
- Designated Safeguarding Lead
- Staff – including Teachers, Support Staff, Technical staff
- Governors with responsibilities for Safeguarding
- Parents and Carers
- Community users

Consultation with the whole school community has taken place through the following:

- Staff meetings / INSET Day
- School elected council members/Equalities Team
- Governors' meeting / committee meetings
- Parents' evenings
- School website / newsletters

The implementation of this e-safety policy will be monitored by: A Smith, the deputy headteacher/Designated Safeguarding Lead.

The Governing Body / Governors Sub Committee will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at full governing body meetings.

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, new threats to e-safety or incidents that have taken place.

Should serious e-safety incidents take place, the Local Authority and the chair of governors will be informed.

The E-Safety Policy should be read alongside the LSCB E-Safety framework (revised December 2015) http://www.bathnes.gov.uk/sites/default/files/sitedocuments/Children-and-Young-People/ChildProtection/e-safety_strategy.pdf

The school will monitor the impact of the policy using:

- Logs of reported incidents
- SWGfL (South West Grid for Learning) monitoring logs of internet activity
- Surveys / questionnaires of pupils
- Parents and Carers
- Staff

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the *Governing Body*	
The implementation of this e-safety policy will be monitored by the:	*Safeguarding Committee*
Monitoring will take place at regular intervals:	*Once a year.(at least)*
The *Governing Body* will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	*Once a year. (at least)* *Summer term*
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, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	July 2016
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*If a child is at immediate risk call the Children and Families Assessment and Intervention Team on 01225 396312 or 01225 396313* *LA E-Safety Statement Author: Richard Baldwin* *LA Designated Safeguarding Officer: Jackie Deas*

Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school / academy ICT systems, both in and out of the school.
The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of children 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 (for example through our use of 3P Learning's Mathletics). The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by a 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 e-safety behaviour that take place out of school.

Roles and responsibilities

As this is a small school many of these roles will be combined.

Governors

Governors are responsible for the approval of the e-safety policy and for reviewing its effectiveness. A member of the Governing Body has taken on the role of Safeguarding Governor. This role will include regular meetings with the E-Safety Co--ordinator and monitoring e-safety incident logs.

Headteacher and Senior Leaders

· The HT is responsible 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.
· The HT / SLT are responsible for ensuring that the E-Safety Coordinator /and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
· The HT/SLT will approach the LA E-Safety office, for advice and support 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. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
· The HT/DHT 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 SWGfL flow chart on dealing with e-safety incidents – in appendix)

E-Safety Coordinator

- 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 school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future esafety developments,
- attends relevant meeting / committee of Governors

ICT Technician : MARCCS Ltd

MARCCS Ltd is responsible for ensuring:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- users may only access the school's networks through a password protection system
- SWGfL is informed of issues relating to the filtering applied by the Grid
- that the IT technician is 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 and email is regularly monitored in order that any misuse /

attempted misuse can be reported to the E-Safety Co-ordinator / Headteacher for investigation.

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use/Password Security and Use of Mobile Phone and Cameras Policies.
- they report any suspected misuse or problem to the E-Safety Co-ordinator / Headteacher / Safeguarding Lead for investigation
- digital communications with children should only be carried out via the school office. Members of staff should not be in communication with current pupils via networking sites.
- e-safety issues will be embedded in the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- 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.
- in lessons where internet use is pre-planned any unsuitable material that is found in internet searches should be initially logged on the incidents form and reported.

Designated Safeguarding Lead

should be trained in e-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

Children

- are responsible for using the school ICT systems in accordance with the Home School agreement
- 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 rules on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school rules 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 / 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. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature.
Parents and carers will be encouraged to support the school / academy 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 records
- their children's personal devices in the school (where this is an agreed practice)

Policy Statements

Education – students / pupils

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

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a programme of assemblies
- Older children 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.
- 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 children 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 children 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, 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 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:

- Curriculum activities
- Letters, newsletters, web site, VLE
- Parents / Carers sessions
- 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

Education and Training – Staff / Volunteers

It is essential that all staff 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.
- The E-Safety Coordinator / Officer (or other nominated person) will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) 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 / team meetings / INSET days.
- The E-Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

Education and Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / e-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 (eg SWGfL).
- 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 network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- 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 academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to technical systems and devices.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password and will be required to change their password every 60 days and not re-use passwords for 6 months.
- The “master / administrator” passwords for the school ICT system, used by the Network Manager must also be available to the *Headteacher* or other nominated senior leader and kept in a secure place (eg school safe)
- The technical managers/Headteacher are 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.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed.
- 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.
- The use of the Google Drive and associated systems is bound by the Google Privacy Policy and Self Regulatory Frameworks (http://www.google.com/policies/privacy/) .
- The Acceptable Use Policy restricts the extent of personal use that users (staff/children/ community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and children 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 children 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 are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents / carers comment on any activities involving other children in digital video images.
- Staff and volunteers are allowed to take digital 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. (as per the Policy on the use of mobile phones and cameras by staff, volunteers and non-staff, and the sharing of images)
- Children must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.
- Children's full names will not be used anywhere on a website or blog, particularly in association with photographs.

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, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software

- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

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:

	Staff & other adults				Students / Pupils			
Communication Technologies	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 mobile phones				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			X				X	

Authorizing Internet Access

All staff must read and sign the Acceptable Use Policy & Staff Code of Conduct for Using ICT and the Appendix relating to the use of Youtube videos before using any school internet resource.

Children should always be supervised by a responsible adult when using the Internet. Teachers should evaluate any websites fully before they use them with their students. Often this means checking the websites, search results etc just before the lesson. What may be considered a safe site today might not be tomorrow. Pay particular attention to image advertisements as they can change each time the web page is accessed.

At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

At Key Stage 2 Children will only be allowed to make searches on 'Google images' when the teacher has already checked the results for such a search. Image searches are especially risky. There may be no need for pupils to download images if an adult downloads them before the lesson and stores them in a shared folder.

Parents & Children will be asked to sign and return a consent form as part of the Home-school agreement.

Any person not directly employed by the school will be asked to sign a **Visitors' Code of Conduct for ICT** proforma before being allowed to access the internet from the school site.

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor B&NES LA can accept liability for any material accessed, or any consequences of Internet access.

The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the headteacher.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of consequences for pupils misusing the Internet.

Introducing the e-safety policy to pupils

E-Safety rules will be posted in all rooms and areas where computers are used and discussed with pupils regularly.

Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

E-Safety teaching is embedded within the Computing Curriculum

Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and have its importance explained and highlighted.

Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

Enlisting parents' and carers' support

Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Web site.

The school will maintain a list of e-safety resources for parents/carers.

The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school

Appendix 1:

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, 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 in 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 or 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.

Students / Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to DTCP – DT e-safety Andrew Wishart	Refer to Headteacher	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	X	X	X
Unauthorised use of non-educational sites during lessons	X	X	X			X	X	X	
Unauthorised use of mobile phone / digital camera / other handheld device	X	X	X			X		X	
Unauthorised use of social networking / instant messaging / personal email	X	X	X			X	X	X	
Unauthorised downloading or uploading of files	X	X	X		X	X	X	X	
Allowing others to access school network by sharing username and passwords	X	X	X			X	X	X	
Attempting to access or accessing the school network, using another student's / pupil's account	X	X	X			X	X	X	
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X		X	X	X	X	
Corrupting or destroying the data of other users	X	X	X		X	X	X	X	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X	X		X	X	X	X	
Continued infringements of the above, following previous warnings or sanctions	X	X	X		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	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X	X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X	X	X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		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

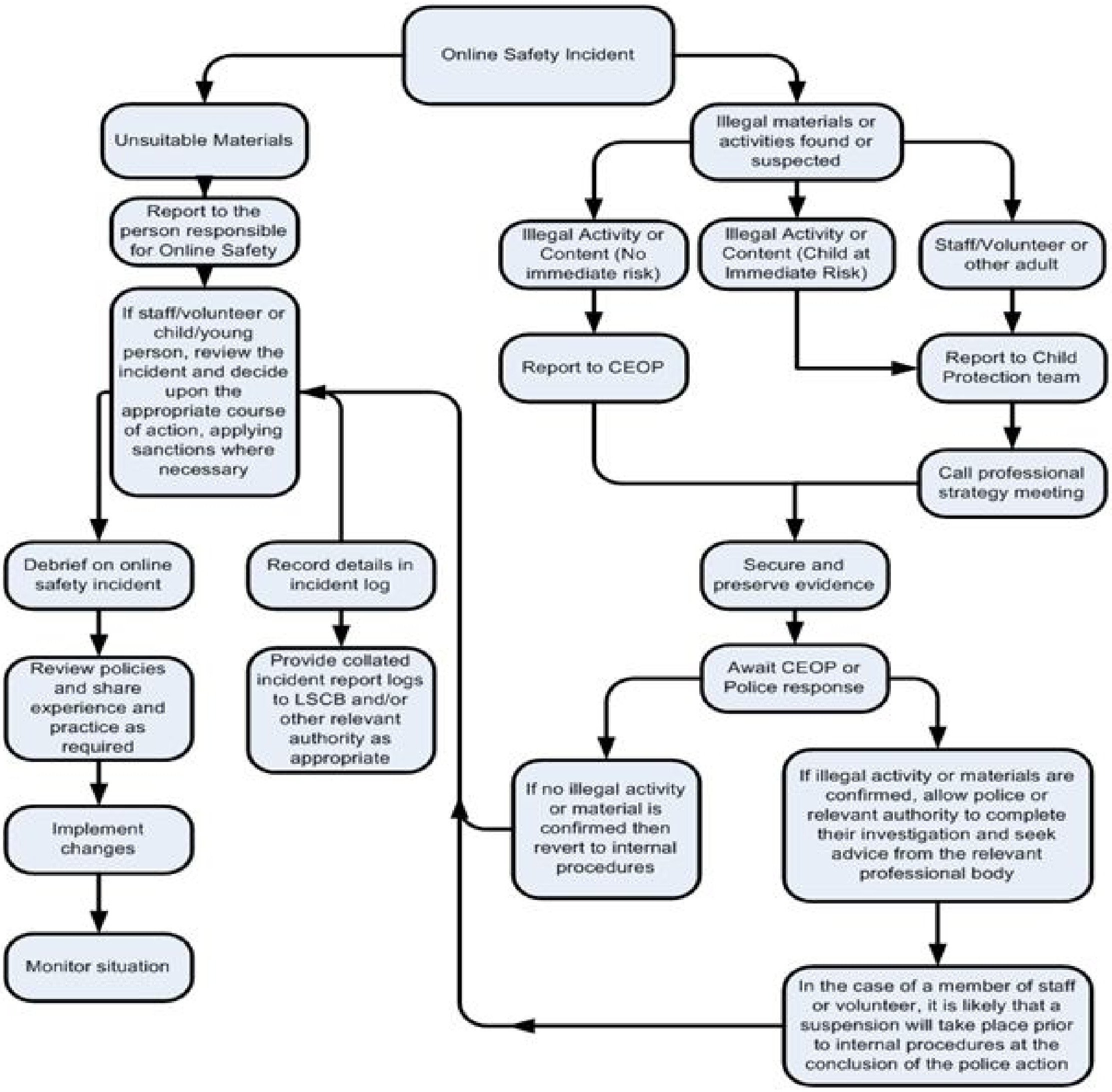
Incidents:	Refer to DT-ESAFETY	Refer to Headteacher	RRefer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X		X	X
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / 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		
Careless use of personal data eg holding or transferring data in an insecure manner	X	X	X		X	X		
Deliberate actions to breach data protection or network security rules	X	X	X		X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X		X	X		X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X	X		X	X		X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X		X	X		X
Actions which could compromise the staff member's professional standing	X	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 filtering system	X	X	X		X	X		X

Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X	X		X	X		
Continued infringements of the above, following previous warnings or sanctions	X	X	X		X	X	X	X

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 CEOPS immediately. Other instances to report to the police would include:**
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *school / academy* and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Implement changes
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Appendix 2: Internet use - Possible teaching and learning activities

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

Reporting Log
Group ....

Date	Time	Incident	Action taken		Incident Reported by	Signature
			What?	By whom?		

Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.
It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject’s rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;

- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:
http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations

Links to other organisations or documents

The following links may help those who are developing or reviewing a school e-safety policy.

UK Safer Internet Centre

Safer Internet Centre -

South West Grid for Learning

Childnet

Professionals Online Safety Helpline

Internet Watch Foundation

CEOP

http://ceop.police.uk/ ThinkUKnow

Others:

INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm

UK Council for Child Internet Safety (UKCCIS) www.education.gov.uk/ukccis

Netsmartz http://www.netsmartz.org/index.aspx

Support for Schools

Specialist help and support SWGfL BOOST

Cyberbullying

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Scottish Government Better relationships, better learning, better behaviour

DCSF - Cyberbullying guidance

DfE – Preventing & Tackling Bullying – Advice to school leaders, staff and Governing Bodies

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm

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

Connectsafely Parents Guide to Facebook

Facebook Guide for Educators

Curriculum

SWGfL Digital Literacy & Citizenship curriculum

Glow - http://www.educationscotland.gov.uk/usingglowandict/

Alberta, Canada - digital citizenship policy development guide.pdf

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Somerset - e-Sense materials for schools

Mobile Devices

Cloudlearn Report Effective practice for schools moving to end locking and blocking

NEN   - Guidance Note - BYOD

Data Protection

Information Commissioners Office:

Your rights to your information – Resources for Schools - ICO

ICO pages for young people

Guide to Data Protection Act - Information Commissioners Office

Guide to the Freedom of Information Act - Information Commissioners Office

ICO guidance on the Freedom of Information Model Publication Scheme

ICO Freedom of Information Model Publication Scheme Template for schools (England)

ICO - Guidance we gave to schools - September 2012 (England)

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Hosted Services

Information Commissioners Office good practice note on taking photos in schools

ICO Guidance Data Protection Practical Guide to IT Security

ICO – Think Privacy Toolkit

ICO – Personal Information Online – Code of Practice

ICO – Access Aware Toolkit

ICO Subject Access Code of Practice

ICO – Guidance on Data Security Breach Management

SWGfL - Guidance for Schools on Cloud Hosted Services

LGfL - Data Handling Compliance Check List

Somerset - Flowchart on Storage of Personal Data

NEN - Guidance Note - Protecting School Data

Professional Standards / Staff Training

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

Kent - Safer Practice with Technology

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

Infrastructure / Technical Support

Somerset - Questions for Technical Support

NEN - Guidance Note - esecurity

Working with parents and carers

SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum

SWGfL BOOST Presentations - parents presentation

Connect Safely - a Parents Guide to Facebook

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

DirectGov - Internet Safety for parents

Get Safe Online - resources for parents

Teach Today - resources for parents workshops / education

The Digital Universe of Your Children - animated videos for parents (Insafe)

Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide

Insafe - A guide for parents - education and the new media

The Cybersmile Foundation (cyberbullying) - advice for parents

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011

Futurelab - "Digital participation - its not chalk and talk any more!"

Approved by the Full Governing Body on:

Review : December 2016

Signed:

Date :