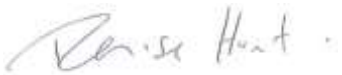
Bournville Primary School E-safety policy

Date Ratified: 24th November 2015

Signed By: 

On behalf of School Governors

Signed by :
Headteacher

Review Date: November 2016

Bournville Primary School- E-safety policy

Rationale

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors and community users) both in school and/or out of school. It is a statement of the aims, principles, strategies and procedures for e-safety throughout the school.

The policy provides the framework to nurture a safe digital community. 'Information Governance' refers to and encompasses the policies, procedures, processes and controls implemented to manage information. These support the school's immediate and future regulatory, legal, risk and operational requirements. Therefore the E-Safety Policy is part of the Information Governance suite and should be read in conjunction with our Data Protection and Information Sharing Policy, Safeguarding Policy and Whistle Blowing Policy.

The following legislation and guidance must be considered when adhering to this policy:

- Obscene Publications Act 1959/1964
- Protection of Children Act 1988/1989
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Defamation Act 1996
- Protection from Harassment Act 1997
- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act (RIPA) 2000
- Safeguarding Vulnerable Groups Act 2006
- Equality Act 2010
- Common law duty of Confidentiality
- Information Sharing Guidance
- Tackling Extremism and Radicalisation

(*Please note this list is intended to be indicative only)*

This E-Safety Policy now includes, as Appendices;

1. Roles and responsibilities
2. Responding to incidents of illegal misuse
3. Unsuitable and inappropriate activities
4. E-Safety contacts and references
5. Legislation
6. E-Safety incident report

What is E-Safety?

E-Safety refers to child protection and safeguarding of both children and adults in the digital world. It is about learning to understand and use technologies in a safe, positive way, also about supporting children and adults to develop safe online behaviours (both in and out of school).

Risks to children who use the internet include:

- Exposure to inappropriate materials, for example, pornographic pictures and videos
- Physical danger and sexual abuse, for example, through 'grooming' by paedophiles
- Obsessive use of the internet and ICT, for example, addiction to video games
- Cyber bullying – persistent bullying through the digital medium
- Inappropriate or illegal behaviour, for example, exposure to hate mail or offensive images
- Copyright infringement, for example, the illegal sharing of music, pictures, video or documents
- Extremism and Radicalisation

There are also risks to staff who use the internet.

E-Safety is largely concerned with internet communications. The internet is accessible from computers, laptops, tablets, mobile phones, games consoles and other devices like the iPod Touch and internet connected TV. Other communication technologies such as texting and phone calls are also covered by the term 'E-Safety'.

Why provide Internet Access?

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience. The internet is part of the statutory curriculum and an entitlement for pupils as part of their learning experience. It is used in this school to raise educational standards, promote pupil achievement and as a necessary tool for staff to support their professional work. The internet also enhances the school's management information and business administration systems.

School Policy on the use of ICT

Internet

- Pupils will be taught what internet use is acceptable and what is not. They will be given clear objectives for internet use.
- School internet access will be filtered appropriate to the ability of the pupils to use it within school rules
- Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity
- Internet access will be planned to enrich and extend learning activities
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation

- Pupils are required to return a signed copy of the ICT Acceptable Usage Agreement for Pupils every year which must be countersigned by their parent or carer

All staff and visitors to school must read and sign the ICT Acceptable Usage Agreement for Staff and Community Users before using any school ICT resources

- Pupils will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable
- Pupils will be taught to question information before accepting it as true
- The school will ensure that use of internet derived materials by staff and pupils complies with copyright law

Email

- Staff and pupils may only use official school email accounts on the school system. Personal email accounts are not to be used.
- All emails sent must be professional in tone and content
- Personal email accounts must not be used for communication between staff and students or parent/carers
- Personal information (as defined in the Personal Data and Information Sharing Policy) must not be emailed to external email addresses from school email accounts as it is not secure.
- Secure email must be used when sending or sharing personal data and information (as defined in the Personal Data and Information Sharing Policy).
- Personal information must not be emailed from staff to the official school email address Bournville.School@n-somerset.gov.uk and vice versa, as it is not secure
- Pupils must have adult supervision whilst using email
- Pupils must immediately tell a teacher if they receive offensive email
- Pupils must not reveal personal details of themselves or others in email communication (such as address or telephone number). Pupils must not arrange to meet anyone without specific permission.
- Email sent to an external organisation should be written carefully and authorised by a member of staff before sending
- The forwarding of chain letters is not permitted
- Pupils will be made aware that the writer of an email (or the author of a web page) may not be the person claimed

Social Networking

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyber bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues

- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Raise any concerns that any colleague(s) is/are not acting in accordance with this Policy with the Headteacher
- Use their professional judgment and, where no specific guidance exists, take the most prudent action possible and consult with the Headteacher if they are unsure
- Co-operate with management in ensuring the implementation of this policy
- Keep a professional distance from pupils and ensure a clear separation of the private social lives of workers at the school and those of pupils.

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

Chatrooms and Instant Messaging

- The use of these facilities is not permitted in school

Video Conferencing and other Video Communications

- Visitors/contributors may be invited to join (supervised) lessons through Skype or video conferencing in accordance with the Visitor to School Policy
- Pupils will not be allowed unsupervised access to video communications

Digital communication may take place between staff and students or parents/carers using only official monitored school systems and must be professional in tone and content. Official school systems include: school email, official Parentmail emails/texts, school website.

Mobiles, cameras and portable digital devices

Pupils:

- Mobile phones, tablets, portable electronic games and media players brought into school by pupils must be handed-in to the class teacher, unless the Headteacher has given permission.
- If children have to bring mobile phones into school for a specific reason such as needing it to walk home after school. Then it will need to be stored in a locked cupboard in the classroom and signed in and out by the class teacher and pupil **(see appendix 7).**
- If a pupil is found to be in possession of one of these electronic devices, the Education Act 2012 gives authorised staff the right to search for such devices (in accordance with school policies) where

they reasonably suspect that the data or files on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules

- The sending of abusive or inappropriate text messages is forbidden

Staff/Visitors/Students/Volunteers/Contractors:

- Use of personal devices in school such as computers, tablets and any other device with the functionality to take pictures, videos or make sound recordings, is not permitted. Exceptions to this rule are personal mobile phones and any device with specific written permission from the Headteacher.

- Staff/Visitors/Students/Volunteers/Contractors may only use personal mobile phones in designated areas. These areas are...
  -School Business Team offices
  -Any rooms within the 'XTND' corridor that are not being used by visitors, staff or children
  -The staff room (not the outside courtyard if children are present)
  -The car park

  2+ nursery – practitioners may only use mobile devices in the kitchen area and the above designated areas in the school.

  During wider community events, assemblies and open morning/afternoons Parents/Carers and visitors are not permitted to take photographs using their own personal mobile phones or other camera devices or use mobile phones.

- Use of personal mobile phones in school must be within the ICT Acceptable Usage Agreement
- Mobile devices must be kept locked in lockers or cupboards.
- Staff/Visitors/Students/Volunteers/Contractors must not keep or use personal mobile phones in view of children
- Staff/Visitors/Students/Volunteers/Contractors must not use personal mobile phones in the vicinity of children (eg if there are pupils in the staff room or offices)
- The sending of abusive or inappropriate text messages is forbidden
- Staff/Visitors/Students/Volunteers/Contractors must not use personal devices to take images of children
- Staff/Visitors/Students/Volunteers/Contractors must not use personal devices to take any images, video or sound recordings in school
- Staff/Visitors/Students/Volunteers/Contractors must not use school devices to take inappropriate images of children or images of children in non-designated areas (non-designated areas include toilets and changing rooms)
- Staff/Visitors/Students/Volunteers are allowed to take digital photographs and video images to support educational aims, but follow guidance in the ICT Acceptable Usage Agreement for Staff and Community Users concerning the taking, sharing, distribution and publication of those images
- Text messaging must not be used for communication between staff and parents unless specific written permission has been obtained from the Headteacher
- Staff who are issued with iPads must sign the appropriate agreement

- All staff have read and agreed to the principles of 'Safer Working Practice'
- Members of staff who have requested to bring their own device to work for school use, have done so with agreement from the head teacher and full knowledge of the school technical support engineer, they adhere to the acceptable use and data protection policies

Memory Sticks and other portable storage

This includes portable USB flash drives and portable hard disk drives.

The Information Commissioner's Office has the power to impose hefty fines on schools and individuals who lose personal data. The loss of an unencrypted memory stick containing the names of pupils would count. There will be sanctions for any breach of this policy.

- Encrypted memory sticks are provided for specific data, this data will not be downloaded to home computers
- Memory sticks or portable hard disk drives may be used in exceptional circumstances with specific written permission from the Headteacher
- Media card readers may be used to retrieve photos and video from school-owned camera cards (eg SD cards)
- The school's Data Protection and Information Sharing Policy applies

Optical Discs

School data in any form (documents, pictures, videos etc) will not be burned to CD or DVD except:

- when archiving data to be stored securely at school
- with specific written permission from the Headteacher

School Website

- The point of contact on the website should be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- Website photographs that include pupils will be selected carefully and will only be published with parental permission
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs
- The Headteacher will delegate editorial responsibility to the School Bursar/Administration support, to ensure that content is accurate and quality of presentation is maintained

Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school is allowed

Cyberbullying

Cyberbullying is the use of the internet and related technologies to harm other people, in a deliberate, repeated, and hostile manner. When children are the target of bullying via mobiles phones, gaming or the internet, they can often feel very alone and, a once previously safe and enjoyable environment or activity, can become threatening, harmful and a source of anxiety.

- Pupils will be taught about the effects of cyberbullying
- Pupils will be encouraged to keep any evidence of cyberbullying

- Pupils will be made aware that the police will be able to trace the originator of any messages
- Cyberbullying (along with all forms of bullying) will not be tolerated in school. All incidents reported will be recorded and investigated.

Filtering

- The school Filtering is provided by SWGfL and formally agreed by the Senior Management.
- Any change requests would need to be managed by the head teacher
- Any changes to the current filtering would need to be undertaken with explicit permission of the head teacher and e-safety group
- The school will work in partnership with the LA, DfE and the Internet Service Provider (South West Grid for Learning) to ensure systems to protect pupils are reviewed and improved
- If staff or pupils discover an unsuitable site, the URL, content, user who made the discovery, time it was discovered and device that was being used must be reported to the E-Safety Co-ordinator/Technical Support and record this in the incident report log. If appropriate, the E-Safety Co-ordinator/Technical Support will inform the Internet Service Provider in order for the site to be blocked. If the material reported is illegal the school will follow the procedure detailed in the incident flow chart. **Appendix 2**

Monitoring

- Logs of internet activity will be regularly checked
- Pupil and staff files stored on school computers will be regularly checked
- Pupil and staff emails will be regularly checked
- Pupil and staff use of social networking websites will be regularly checked
- Illegal misuse will be dealt with in accordance with the procedure detailed in **Appendix 2**

School ICT and Data Security

- The school Data Protection and Information Sharing Policy applies
- The school Password Security, Filtering and the ICT Service Continuity Management requirements apply

- A safe and secure username/password system is essential and will apply to all school technical systems, including networks, devices, email and virtual learning environment (VLE).
- Passwords must be changed every 90 days - enforced to change.
- Passwords must be secure and recommended to consist of uppercase character, lowercase character, number, special character.
- Passwords should be different for different accounts to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school.
- Pupils will be taught the importance of password security through the curriculum and acceptable use agreements.
- Users must not share their user account details and must not leave their computers unlocked and accessible to others
- An agreed process being in place for the provision of temporary access of “guests” (e.g. trainee teachers, visitors) onto the school system. All

"guests" must sign the staff AUP and are made aware of this e-Safety policy
- Administrative data sent over the internet will be encrypted or otherwise secured
- Unapproved system utilities and executable files are not permitted on school equipment
- No school data (pictures, videos, documents etc) other than that which is freely accessible on the school website, is to be stored on any computer other than those owned by the school
- Loss of personal data must be immediately reported to the Headteacher, as an Information Risk Incident.
- Virus protection updates and system updates for PCs will be regularly installed
- School ICT systems security will be reviewed regularly

Policy Enforcement

The E-Safety Co-ordinator will ensure that the E-Safety Policy is implemented and compliance with the policy monitored. **Appendix 3** shows which activities are deemed 'Acceptable' or 'Unacceptable'.

Any unacceptable or illegal activities will result in disciplinary procedures being instigated.

Pupils:

- All pupils and their parents/carers must sign the ICT Acceptable Usage Agreement for Pupils every year
- The ICT Acceptable Usage Agreement for Pupils will often be referred to in lessons
- E-Safety rules will be posted in all rooms where computers are used and will be discussed with pupils at the start of each academic year
- Pupils will be informed that internet use will be monitored and sanctions will be imposed if the facility is abused
- Any breaches of the ICT Acceptable Usage Agreement for Pupils will be referred directly to the E-Safety Co-ordinator
- The school will keep a record of all pupils who have been denied internet access and the reason and length of time it was denied
- Pupils will be informed that network and internet use will be monitored
- Instruction in responsible and safe use will precede internet access
- Pupils' work will only be published with the permission of the pupil and parents

Staff:

- All staff must read and sign the ICT Acceptable Usage Agreement for Staff and Community Users before using school ICT resources and annually thereafter
- The school will keep a record of all staff who have been denied internet access and the reason and length of time it was denied

- All staff including teachers, supply staff, teaching assistants and support staff, will be provided with this e-Safety Policy, and its importance will be explained
- Staff will be made aware that professional conduct is essential when using school ICT and that internet use will be monitored and can be traced to the individual user
- Any breaches of the ICT Acceptable Usage Agreement for Staff will be referred directly to the Headteacher
- Implementation of the e-Safety rules will be checked regularly by the E-Safety Co-ordinator
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective

Complaints

- Responsibility for handling incidents of internet misuse will be taken by the E-Safety Co-ordinator
- Any complaint about staff misuse of ICT must be referred to the Head teacher
- Complaints of a child protection nature must be dealt with in accordance with school safeguarding procedures
- Pupils and parents will be informed of the complaints procedure
- Parents and pupils will need to work in partnership with staff to resolve issues
- There may be occasions when discussions will be held with the police support services to establish procedures for handling potentially illegal issues
- Where possible the school will liaise with local organisations to establish a common approach to e-safety
-

Parental Support

- Parents' attention will be drawn to the school E-Safety Policy in newsletters, the school website, during e-safety events and during the annual e-safety week, parents evening, social media.
- Parents will be asked to read through the ICT Acceptable Usage Agreement for Pupils with their child and co-sign the agreement
- Internet issues will be handled sensitively to inform parents without undue alarm
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe internet use at home.

Education

Education & Training: Staff and Governors

There is a planned programme of e-safety training for all staff and governors to ensure they understand their responsibilities, as detailed in this, and the ICT Acceptable Usage Agreement for Staff and Community Users.

- An audit of the e-safety training needs of all staff is carried out annually
- All new staff receive e-safety training as part of their induction programme
- The E-Safety Co-ordinator receives regular updates through attendance at SWGfL, CEOP, LA training sessions and by reviewing regular e-safety updates from the local authority

- This E-Safety Policy and its updates are shared and discussed in staff meetings. Updates are provided to all staff.
- The E-Safety Co-ordinator provides advice/guidance and training as required and seeks LA advice on issues where required.

Education: Pupils

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

- There is a planned e-safety scheme of work
- Key e-safety messages are reinforced annually through an assembly and e-safety week
- Pupils are helped to understand and act in accordance with the ICT Acceptable Usage Agreement for Pupils
- Pupils are taught to acknowledge the sources of information they use and to respect copyright when using material accessed on the internet
- The ICT Acceptable Usage Agreement for Pupils is displayed in all rooms where ICT is used
- E-safety is a focus in all relevant areas of the curriculum
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and 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, e.g. using search engines, staff are vigilant in monitoring the content of the websites the young people visit and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material
- Students are taught to be critically aware of the materials / content they access online and be guided to validate the accuracy of information
- When using digital images, pupils are taught about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites
- Staff act as good role models in their own use of ICT
- Staff are familiar with and ensure that pupils act in accordance with the ICT Acceptable Usage Agreement for Pupils

Education: Parents/Carers

Parents and carers may have only a limited understanding of e-safety issues and may be unaware of risks and what to do about them. However, they have a critical role to play in supporting their children with managing e-safety risks at home, reinforcing key messages about e-safety and regulating their home experiences. The school supports parents to do this by:

- Providing regular newsletter and website updates on e-safety
- Proving information leaflets to parents
- Inviting parents to attend activities such as e-safety sessions
- Promoting e-safety at Parents Evenings

Risk

The school will take all reasonable steps to mitigate the risks identified above and ensure that users create and access only appropriate 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 school computer. An E-Safety Co-ordinator has been appointed to oversee internet dangers, risk assessment and matters arising from internet use. However, neither the school nor North Somerset Council can accept liability for the material accessed, or any consequences of internet access.

Development, monitoring and review of the policy

This e-safety policy has been developed, and will be monitored, by our school e-Safety Committee which comprises:

- Headteacher
- E-Safety Co-ordinator
- ICT Co-ordinator
- E-Safety Governor
- Teaching and Support staff
- Parent representative
- Local PCSO
- Consultation with the whole school community has taken place through staff meetings, Student Council meetings, Governors meetings, E-Safety Week and the school newsletter.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- SWGfL monitoring logs of internet activity
- Other internal monitoring data
- Surveys of students, parents/carers and staff (including non-teaching staff)
- Regular checks on school emails, users' files, browsing history and staff and pupil use of social networking websites

The policy will be reviewed immediately where monitoring data shows a need. The policy will also be reviewed annually.

Appendix 1

Roles and responsibilities

The Headteacher is responsible for ensuring the safety (including e-Safety) of all members of the school community, though the day to day responsibility for e-Safety can be delegated.

The e-Safety Leader, working with the designated Child Protection Coordinator will have overview of the serious child protection issues to arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate on-line contact with adults, potential or actual incidents of grooming and cyber-bullying.

An e-Safety committee will work with the e-Safety Leader to implement and monitor the e-Safety policy and AUPs (Acceptable User Policies). This group is made up of e-Safety Leader, Child Protection Coordinator, teacher, governor, member of support staff, technician, member of senior leadership team and pupils. Pupils are part of this group, working with them through the school council, to contribute their knowledge and use of technology. They meet three times a year (terms 2, 4 and 6).

Role	Responsibility
Governors	• Approve and review the effectiveness of the e-Safety Policy • Delegate a governor to act as e-Safety link • e-Safety Governor works with the e-Safety Leader to carry out regular monitoring and report to Governors
Head Teacher and Senior Leaders	• Ensure that all staff receive suitable CPD to carry out their e-Safety roles • Create a culture where staff and learners feel able to report incidents • Ensure that there is a system in place for monitoring e-Safety • Follow correct procedure in the event of a serious e-Safety allegation being made against a member of staff or pupil • Inform the local authority about any serious e-Safety issues • Ensure that the school infrastructure/network is as safe and secure as possible • Ensure that policies and procedures approved within this policy are implemented • Use an audit to annually review e-Safety with the school's technical support

e-Safety Leader	• Lead the e-Safety committee • Log, manage and inform others of e-Safety incidents • Lead the establishment and review of e-Safety policies and documents • Ensure all staff are aware of the procedures outlined in policies relating to e-Safety • Provide and/or broker training and advice for staff • Attend updates and liaise with the LA e-Safety staff and technical staff • Meet with Senior Leadership Team and e-Safety Governor to regularly discuss incidents and developments • Coordinate work with the school's designated Child Protection Coordinator

Appendix 2

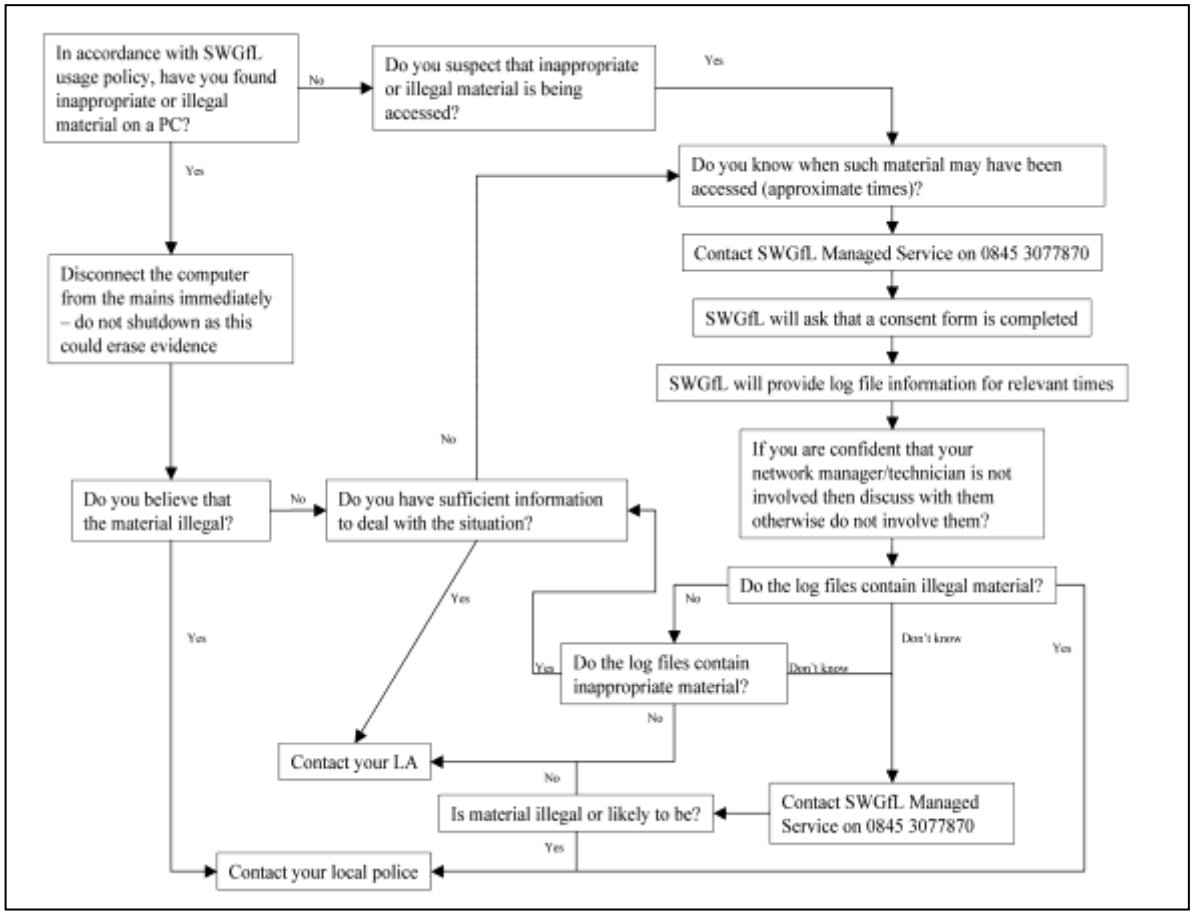
Responding to incidents of misuse

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 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 i.e.

- 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:

If an incident or concern needs to be passed beyond the school then the concern will be escalated to the Safeguarding for Schools Adviser to communicate to other schools in Somerset. **Should serious e-Safety incidents take place, the following external persons and agencies should be informed:**	**Safeguarding for Schools Adviser** **Local Authority Designated Officer (LADO)** ***where staff involved*** **Police** **ICT LA contact**

Appendix 3

User Actions		Acceptable	Acceptable with permission certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**child sexual abuse images**					✓
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
	adult material that potentially breaches the Obscene Publications Act in the UK					✓
	criminally racist material in UK					✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred				✓	
	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					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
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					✓	

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				✓					
On-line gaming (educational)			✓						
On-line gaming (non educational)				✓					
On-line gambling				✓					
On-line shopping / commerce		✓							
File sharing				✓					
Use of social networking sites		✓							
Use of video broadcasting eg Youtube		✓							

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	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).		✓	✓	✓					
Unauthorised use of non-educational sites during lessons	✓					✓			
Unauthorised use of mobile phone / digital camera / other handheld device		✓	✓			✓			
Unauthorised use of social networking / instant messaging / 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 instant 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 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			✓			✓			

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓	✓		✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / 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 instant 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 students / 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		✓				✓		
Using proxy sites or other means to subvert the school'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		✓			✓		✓	✓
Breaching copyright or licensing regulations		✓				✓		
Continued infringements of the above, following previous warnings or sanctions		✓					✓	✓

Appendix 4

E-SAFETY CONTACTS AND REFERENCES

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

Appendix 5

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.

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.

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).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

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 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.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

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. (see template policy in these appendices and for DfE guidance - 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

Bournville
PRIMARY SCHOOL

Selworthy Road
Weston Super Mare
BS23 3ST
Tel: 01934 641783
Fax: 01934 644502
www.bournville.org

E-safety Incident Sheet

Use this sheet to record any incidents which you are aware of that are a cause for concern

Child Concerned	
Date of Report	
Reported by	

Details: State clearly what happened. Note any school equipment that may need checking. Note any internet sites etc that may be relevant.

Action Taken
By whom
Follow Up if Needed

Appendix 7

Teacher and child to both sign in and out.

Children's Mobile Phone Sign In and Out Log						
Child's Name	Date	Phone model	Signed in	Time	Signed out	Time