Witchampton CofE First School

E-Safety and IT Acceptable Use Policy

As a Church of England School we are guided by our Christian values in supporting the learning of all our children.

Quick Reference:

School E-Safety Policy

1.0 Background/Rationale:

New technologies have become integral to the lives of children in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children should have an entitlement to safe internet access at all times.

E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face by using digital devices, being online and through social media include:

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

Witchampton CofE First School is committed to safeguarding its pupils. Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore vital, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

2.1 Development / Monitoring / Review of this Policy:

This e-safety policy has been developed in conjunction with:

- *School E-Safety Champion*
- *Head of School / Subject Leadership Team (SLT)*
- *Teachers*
- *Support Staff*
- *Governors*

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

- *Staff meetings*
- *School Council*

- *Governors meeting*

Our E-Safety Policy has been agreed by the staff and approved by governors.

2.2 Schedule for Development / Monitoring / Review:

The school E-safety Policy will be reviewed annually.

The school will monitor the impact of the policy using:

- *Logs of reported incidents placed on My Concern*
- *SWGfL monitoring logs of internet activity (including sites visited)*
- *Internal monitoring data for network activity*
- *Surveys / questionnaires of pupils (e.g. Ofsted "Tell-us" survey / CEOP ThinkUknow survey)*
- Parents / carers
- Staff

3.0 Scope of the Policy:

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

The Education and Inspections Act 2006 empowers Head Teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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

4.0 Roles and Responsibilities:

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

4.1 Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of *Safeguarding Governor*. The role of the Safeguarding Governor will include:

- *regular meetings with the E-Safety Champion*
- *regular monitoring of e-safety incident logs*
- *reporting to relevant Governors meeting*

4.2 Head of School and Designated Safeguard Lead (DSL):

- The Head of School (who is the DSL) 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 Champion.
- The Head of School is responsible for ensuring that the E-Safety Champion 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 Head of School will 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 Head of School will receive termly monitoring reports from the E-Safety Champion.
- The Head of School and the Deputy DSL 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 – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures).

4.3 E-Safety Champion:

- Takes day to day responsibility for monitoring e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with the WAT.
- Liaises with school ICT technical staff.
- Liaises with other outside agencies such as the SWGFL and SSCT.
- Receives reports of e-safety incidents via MyConcern and creates a log of incidents to inform future e-safety developments.
- Meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs.
- Reports termly to the Head of School who reports termly to the full governing body.

4.4 Technical staff: Lexicon and D.C.C.:

Lexicon (pupils) and D.C.C (office) is responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant latest update of keeping children safe in education.
- That users may only access the school's networks through a properly enforced password protection policy.
- SWGfL is informed of issues relating to the filtering applied by the Grid.
- The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- That the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head of School / E-Safety Champion / SLT / DSL / Class teacher for investigation / action / sanction.
- That monitoring software / systems are implemented and updated as agreed in school policies.

4.5 Teaching and Support Staff:

are responsible for ensuring that:

- All staff must read and sign the 'Acceptable ICT Use Agreement.'
- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They report any suspected misuse or problems by staff or pupils to the E-Safety Champion/ Head of School/ Class teacher for investigation / action / sanction.
- E-safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the school e-safety policy.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- They monitor ICT activity in lessons, extra-curricular and extended school activities.
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Remote access to the school server is done safely and without breaching the Data Protection Act 1998. Confidentiality of staff and pupil information should be treated the same as if in the school building.

4.6 Designated Safeguarding Lead:

should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- social media
- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- sexting
- radicalisation
- child sexual exploitation

4.7 Pupils:

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- Are educated on safe usage of social media / cyberbullying/ sexting/ grooming/ CSE/ radicalisation /digital social etiquette.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking and the use of images.
- 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.

4.8 Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' campaigns / literature. Parents and carers will be responsible for:

- Their child's use of digital technology outside of school.
- Endorsing (by signature) the Pupil Acceptable Use Policy.
- Accessing the school website / on-line pupil records in accordance with the relevant school Acceptable Use Policy.

5.0 Policy Statements

5.1 Education – pupils:

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

- A planned e-safety programme should be provided as part of Computer Science/ PSHE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

5.2 Education – parents / carers:

Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

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

- Letters, newsletters, website.
- Parents evenings.
- Parent sessions with DSST.
- Reference to the SWGfL Safe website (e.g. the SWGfL "Golden Rules" for parents).

5.3 Education & Training – Staff:

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:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy.

- The E-Safety Champion will receive regular updates through attendance at SWGfL / LA / other information /training sessions and by reviewing guidance documents released by DSST/ SWGfL / LA and others.

- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.

- The E-Safety Champion (or other nominated person) will provide advice / guidance / training as required to individuals as required.

- Follow up training will be provided to staff when the DSL/E-safety Champion have been on relevant courses.

5.4 Training – Governors:

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are responsible for overseeing ICT / e-safety / health and safety / child protection.

This may be offered in a number of ways:

- Attendance at training provided by the Trust / Local Authority / National Governors Association / SWGfL or other relevant organisation.
- Participation in school training / information sessions for staff or parents.

6.0 Technical – infrastructure / equipment, filtering and monitoring:

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that 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.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the E-safety Champion and will be reviewed, at least annually, by the Head of School.
- All users will be provided with a username and password by the Office Administrator who will keep an up to date record of users and their usernames.
- The "master / administrator" passwords for the school ICT system, used by the Office Administrator (or other person) must also be available to the Head of School or other nominated senior leader and kept in a secure place (e.g. school safe).
- Users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security.
- Lexicon maintains and supports the managed filtering service provided by SWGfL.
- In the event of the Office Administrator (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head of School.
- Any filtering issues should be reported immediately to Lexicon.
- Requests from staff for sites to be removed from the filtered list will be considered by the Head of School. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Office Administrator.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view user's activity
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Office Administrator or Head of School.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
- An agreed policy is in place regarding the downloading of executable files by users
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- Personal data such as pupil records must not be kept on laptops and should only be accessed via the secure school server.

- An agreed policy is in place that allows staff to / forbids staff from installing programmes on school workstations / portable devices.
- Memory sticks should not be used unless transferring files to a non-networked machine such as for assembly
- The school infrastructure and individual workstations are protected by up to date virus software.
- Instances of hacking or viruses, such as ransomware, must be reported immediately to the Head of School, Office Administrator or E-safety Champion. This includes outside of school if the remote access is likely to have been compromised.

7.0 Curriculum:

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, 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 (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that Lexicon 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.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

8.1 Use of digital and video images - Photographic, Video:

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social media.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. These images should only be taken on school equipment unless there is no alternative. In this instance direct permission must be been gained from the Head of School and all necessary precautions taken, such as no wi-fi enabled devises, all images to be removed and placed on the school network immediately after use, no images stored elsewhere.
- Only under extreme circumstances may images be taken on personal equipment without prior permission, such as pupil's safety being at risk. The Head of School or Office Administrator must be informed directly after the event.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images (See Official Website Policy).
- Images can only be taken off site and used for educational purposes associated with the school.
- Images should be kept on school owned computers and devices, unless there is no alternative available. In this instance permission must be sort from the Head of School and the images must be removed as soon as possible.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website and in Newsletters.

- Pupil's work can only be published with the permission of the pupil and parents or carers (See Official Website Policy).

8.2 Use of Smart Technology:

Smart technology implies the use of devices using mobile operating systems, such as tablets, phones and watches. These are becoming increasingly prevalent in the classroom. The use of phones, tablets and watches by pupils during school time is prohibited without permission of a teacher. The following rules apply to all members of staff or those working with children at Witchampton:

- Personal use of smart technologies is prohibited during lessons or in front of pupils.
- The use of smart technologies around pupils must be justifiable for educational purposes and included in planning where possible.
- Smart watches may be worn by members of staff, but must not have an inbuilt camera function.
- No personal devices should be used by pupils, unless specific permission has been given by a member of staff.
- If permission has been given for pupils to use their own smart devices, it is the responsibility of the member of staff to remind pupils that the school holds no liability as issued in the home school agreement.
- If required, the school maintains the right to examine any smart technology used on the premises.
- If the personal use of smart technologies is considered or suspected of placing pupils' safety at risk, the police will be informed.
- If permission is given for a pupil to use their own smart device, including e-readers, these should not be internet enabled through 3G, 4G or equivalent.
- Members of staff who have a 3G/4G enabled device should only use these networks when there is no secure school wi-fi signal available.

9.0 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.
- If leaving a computer for any duration it should be locked.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system:

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus 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.

10.0 Communications :

This is an area of rapidly developing technologies and uses. 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				Pupils			
Communication Technologies	Allowed	Allowed at certain times & certain places	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
Smart watches may be bought to school	X						X	
Use of smart watches in lessons				X				X
Use of smart watches in social time		X						X
Taking photos on a smart watch				X				X
Use of hand held devices e.g. e-readers, PDAs.	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	

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored.

- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers (email, school text etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications (See Social Networking Policy).
- Whole class or group email addresses will be used in Y3- Y4 for educational use.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

11.1 Unsuitable / inappropriate activities (Appendix A):

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal, but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**child sexual abuse images**					X
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					X
	adult material that potentially breaches the Obscene Publications Act in the UK					X
	criminally racist material in UK					X
	pornography				X	
	promotion of any kind of discrimination				X	
	promotion of racial or religious hatred					X
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	

Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school				X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					X
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X
Creating or propagating computer viruses or other harmful files				X	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce		X			
File sharing				X	
Use of social networking sites			X		
Use of video broadcasting e.g. YouTube		X			

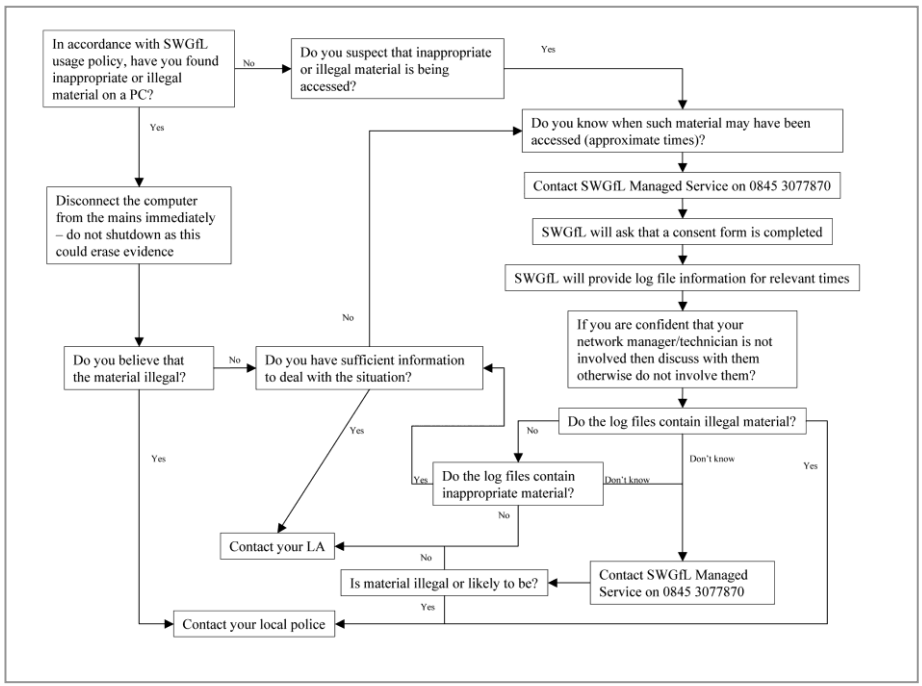
11.2 Responding to incidents of misuse:

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://swgfl.org.uk/FAQs 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:

Pupils	Actions / Sanctions								
Incidents:	Refer to class teacher	Refer to E-safety Champion	Refer to Head of School	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 e.g. 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
Unauthorised use of non-educational sites during lessons	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	
Unauthorised downloading or uploading of files		X	X		X	X		X	X
Allowing others to access school network by sharing username and passwords	X	X	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	X
Corrupting or destroying the data of other users	X	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	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

Using proxy sites or other means to subvert the school's filtering system		X	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
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X	X	X	X	X	X	X

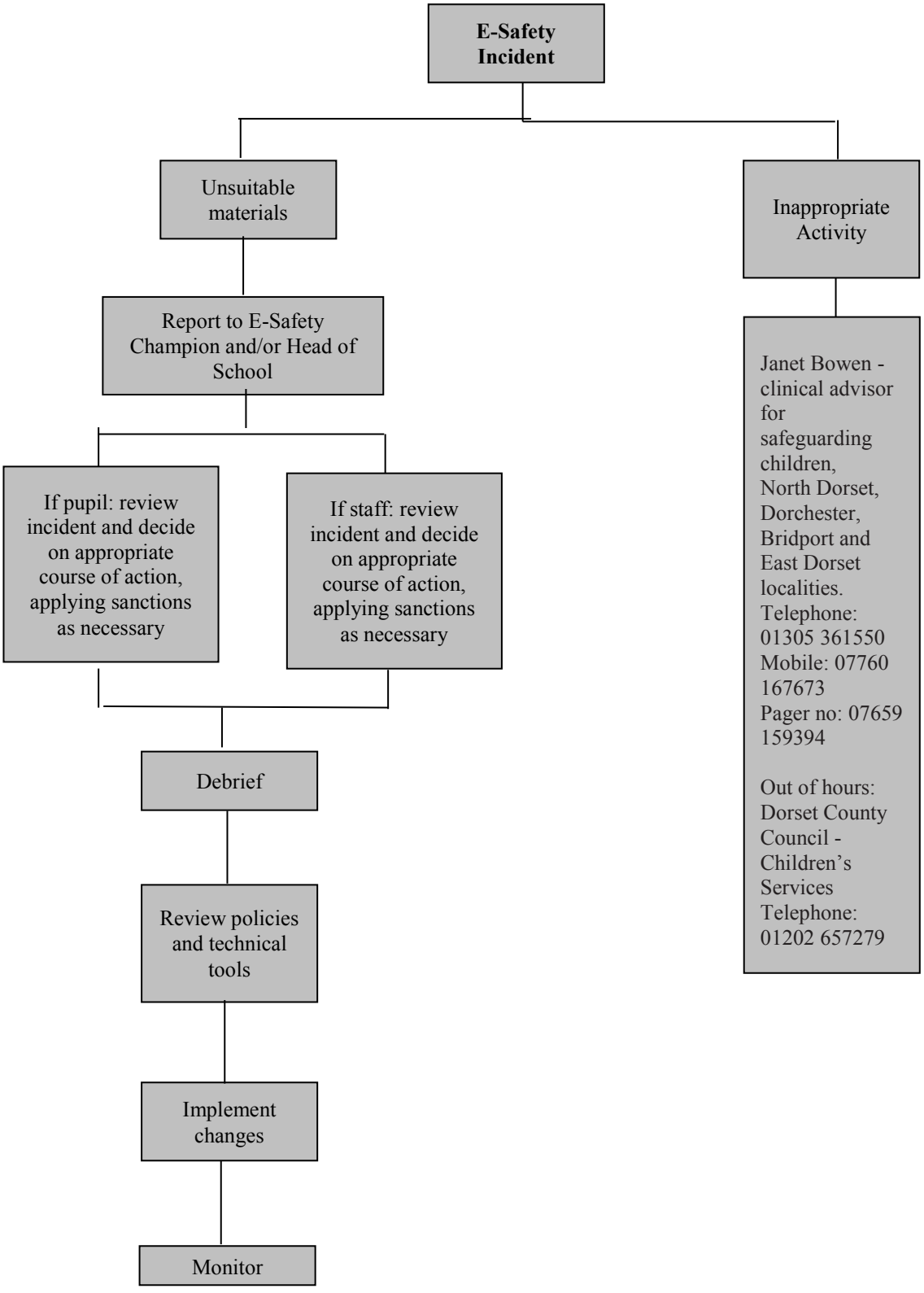
Staff Actions / Sanctions

Incidents:	Refer to E-safety Champion	Refer to Head of School	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action	Refer to DSL
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
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		X	X		X	X	X	X	X
Unauthorised downloading or uploading of files	X	X	X	X	X	X	X	X	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X			X	X			X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X					X			X
Deliberate actions to breach data protection or network security rules		X	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	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X	X	X	X	X	X	X
Actions which could compromise the staff member's professional standing	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
Using proxy sites or other means to subvert the school's filtering system	X				X	X			

Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X			
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X	X	X	X
Breaching copyright or licensing regulations		X	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

Appendix A

Flowchart for responding to e-safety incidents in school



Adapted from Becta – E-safety 2005

Acknowledgements:

Witchampton CofE First School would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School E-Safety Policy Template:

- Members of the SWGfL E-Safety Group and the SWGfL E-Safety Conference Planning Group
- Avon and Somerset Police
- Somerset County Council
- Plymouth City Council
- Swindon Borough Council
- Poole Borough Council
- Bournemouth Borough Council
- North Somerset Council
- Gloucestershire County Council
- DCSF
- Becta
- National Education Network (NEN)
- London Grid for Learning
- Kent County Council
- Northern Grid for Learning
- Bracknell Forest Borough Council
- Byron Review – Children and New Technology – “Safer Children in a Digital World”
- Allenborne Middle School

Date on which policy was approved:

Policy review date: