Original Date Written	Date Reviewed	Date Ratified	Date for Review
November 2016		December 2016	December 2017

Marlborough St Mary’s CE VC Primary School

MARLBOROUGH
ST MARY’S
PRIMARY SCHOOL

E-Safety Policy

MARLBOROUGH ST MARY'S PRIMARY SCHOOL

E-Safety Policy

1. Leadership and Management

1.1 Who will write and review the policy?

The school e-safety policy will feature as part of the review process within the School Development Plan. It should relate to other policies including those for behaviour, for personal, social and health education (PSHE), for bullying and for citizenship.

- *Our e-safety has been written by the school, building on the Wiltshire e-safety template policy and government guidance. It has been agreed by the senior management and approved by governors. It will be reviewed annually.*

1.2 How will Internet access be authorised?

Internet access for pupils should be seen as an entitlement on the basis of educational need and an essential resource for staff. Parental permission will be sought when each pupil starts at St Marys. SWGfL proactively monitors Internet usage for illegal (attempted access of child abuse and incitement for racial hatred) websites and will notify the local police and Wiltshire Council in these instances.

- *The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date; for instance if a pupil's access is withdrawn.*
- *When children start school parents are asked to give written permission for their them to use the internet and for children's pictures to be used on the school Website*
- *Access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials.*
- *Parents will be informed that pupils will be provided with supervised Internet access (an example letter for primary schools is included in The Wiltshire E Safety Toolkit).*

1.3 How will filtering be managed?

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Levels of access and supervision will vary according to the pupil's age and experience. Internet access must be appropriate for all members of the school community from youngest pupil to staff.

- *A designated member of staff will review the popular permitted and banned sites accessed by the school.*
- *The school will work in partnership with parents; Wiltshire Council, DFE and the SWGfL to ensure systems to protect pupils are reviewed and improved.*
- *If staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the Internet Service Provider (SWGfL) via the E-safety lead. (See The Wiltshire E Safety Toolkit for contact details).*
- *Website logs will be regularly sampled and monitored.*
- *Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.*
- *Any material that the school believes is illegal must be referred to the Internet Watch.*

1.4 How will the risks be assessed?

As the quantity and breadth of the information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will address the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system.

- *In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users 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. Neither the school nor Wiltshire Council can accept liability for the material accessed, or any consequences of Internet access.*
- *The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.*
- *Methods to identify, assess and minimise risks will be reviewed regularly.*
- *The head teacher will ensure that the Code of Conduct is implemented and compliance with the policy monitored.*

2. Teaching and Learning

2.1 Why is Internet use important?

The Internet is an essential resource to support teaching and learning. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.

- *Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.*
- *The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, well being and to support the professional work of staff and to enhance the school's management information and business administration systems.*
- *The Internet is an essential part of everyday 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.*
- ***Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.***

2.2 How will Internet use enhance learning?

Benefits of using the Internet in education include:

- *Access to worldwide educational resources including museums and art galleries;*
- *Inclusion in the National Education Network which connects all UK schools;*
- *Educational and cultural exchanges between pupils worldwide;*
- *Vocational, social and leisure use in libraries, clubs and at home;*
- *Access to experts in many fields for pupils and staff;*
- *Professional development for staff through access to national developments,*
- *Educational materials and effective curriculum practice;*
- *Collaboration across networks of schools, support services and professional associations;*
- *Improved access to technical support including remote management of networks and automatic system updates;*
- *Access to learning wherever and whenever convenient.*

2.3 How will pupils learn to evaluate Internet content?

Information received via the web, e-mail or text message requires good information-handling and digital literacy skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.

Ideally inappropriate material would not be visible to pupils using the web but this is not easy to achieve and cannot be guaranteed. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

- *Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.*
- *Pupils will use age-appropriate tools to research Internet content.*
- *The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.*

- *If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the South West Grid for Learning*
- *Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.*
- *Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.*

3. Communication and Content

3.1 Website content

Publication of any information online should always be considered from a personal and school security viewpoint. Sensitive information may be better published in the school handbook or on a secure online area which requires authentication. Editorial guidance will help reflect the school's requirements for accuracy and good presentation.

- *The point of contact on the school website should be the school address, school e-mail and telephone number. Staff or pupils' personal information will not be published.*
- *Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Photographs will be selected carefully and will not enable individual pupils to be clearly identified or include any of those children without permission to be published (whole school list to be kept with superadmin)*
- *Pupils' full names will not be used anywhere on the website, particularly in association with photographs.*
- *The nature of all items uploaded will not include content that allows the pupils to be identified.*
- *The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.*
- *The website should comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.*

3.2 Learning Platforms

Our learning platform offers St Mary's Infant school a wide range of benefits to teachers, pupils and parents, as well as support for management and administration.

- *SLT and staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.*
- *Pupils/staff will be advised about acceptable conduct and use when using the LP.*
- *Only members of the current pupil, parent/carers and staff community will have access to the LP.*
- *All users will be mindful of copyright issues and will only upload appropriate content onto the LP.*
- *When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.*

3.3 Managing e-mail

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects between schools. However, the use of e-mail requires appropriate safety measures.

Schools will need to determine the best approach for their circumstances, based upon pupil age and curriculum requirements. The use of email identities such as john.smith@school.wilts.sch.uk generally needs to be avoided for younger pupils, as revealing this information could potentially expose a child to identification by unsuitable people.

- *Pupils may only use approved e-mail accounts on the school system.*
- *Pupils must immediately tell a responsible adult if they receive offensive e-mail.*
- *Staff will use official school provided email accounts*
- *Pupils should use email in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of school conduct and will be dealt with accordingly.*
- *E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.*

3.4 On-line communications, social networking and social media.

On-line communications, social networking and social media services are filtered in school by the SWGfL but are likely to be accessible from home.

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. Schools have a key role to teach young people about the importance of keeping personal information safe.

- *Students / pupils will be taught about how to keep personal information safe when using online services. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.*
- *Pupils must not reveal personal details of themselves or others in online communication, or arrange to meet anyone.*
- *Social Media tools will not be used with students as part of the curriculum.*
- *Staff official blogs or wikis should be password protected and run with approval from the SLT.*
- *Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.*
- *Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private when using social networking sites at home,*
- *All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.*
- *Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.*
- *Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Code of Conduct.*
- *In line with, 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' it will not be considered appropriate for staff to engage in personal online communications with children and young people, parents or carers. Express care is also to be taken regarding the use of social networking sites.*

3.5 Mobile phones and personal devices

Children are not normally allowed to bring mobile phones into school (Any phones brought into school must be left in the school office).

Use of mobile phones and personal devices by adults are allowed with the following conditions:

- *The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community.*
- *School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.*
- *Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.*
- *Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items.*
- *Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms or toilets.*
- *Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.*
- *Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.*

3.6 Video Conferencing

Videoconferencing enables users to see and hear each other between different locations. This ‘real time’ interactive technology has many potential benefits in education.

- *Videoconferencing will be supervised appropriately for the pupils’ age and ability.*
- *Staff must refer to the internet consent agreements prior to children taking part in videoconferences.*
- *All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.*

3.7 Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom use to be developed. The safest approach is to deny access until a risk assessment has been completed and safety has been established.

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

3.8 Cyberbullying

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Cyberbullying can be defined as “The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone” DCSF 2007. DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying

- *Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school’s policy on anti-bullying and behaviour.*
- *There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.*
- *There are clear procedures in place to support anyone in the school community affected by cyberbullying.*
- *All incidents of cyberbullying reported to the school will be recorded.*
- *The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.*
- *Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school’s e-Safety ethos.*

3.9 Data Protection

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

Schools will already have information about their obligations under the Act, and this section is a reminder that all data from which people can be identified is protected. For advice and guidance relating to a contravention of the Act, contact www.wiltshire.gov
Wiltshire council guidance for schools here:

- *Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.*

4 Implementation

4.1 Introducing the Policy to Pupils

Many pupils are very familiar with Internet use and the culture that surrounds it. As part of the school's e-safety teaching and awareness-raising it is important to discuss the key features with pupils / students as appropriate for their age. Pupils may need to be reminded of the school rules at the point of Internet use.

- *All users will be informed that network and Internet use will be monitored.*
- *An e–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils- See APPENDIX 1.*
- *Pupil instruction regarding responsible and safe use will precede Internet access.*
- *An e–Safety module will be included in the PSHE and/or ICT programmes covering both safe school and home use.*
- *E-Safety rules will be posted in all rooms with Internet access.*
- *Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.*

4.2 Consulting with Staff

It is important that all staff feel confident to use new technologies in teaching and the School e–Safety Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies.

All staff must understand that the rules for information systems misuse for Wiltshire Council employees are specific and that instances resulting in disciplinary procedures and dismissal have occurred. If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with their line manager to avoid any possible misunderstanding.

Particular consideration must be given when members of staff are provided with devices by the school which may be accessed outside of the school network. Schools must be clear about the safe and appropriate uses of their school provided equipment and have rules in place about use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of school information.

- *The e–Safety Policy will be formally provided to and discussed with all members of staff.*
- Staff should be aware that Internet traffic is monitored and reported by the SWGfL and can be traced to the individual user. Discretion and professional conduct is essential.
- *All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.*

4.3 Parents and E-Safety

Parents need to be aware of the potential dangers that are associated with online communications, social networking sites and mobile technologies to help ensure their children are not putting themselves at risk.
Schools may wish to refer parents to websites referred to in the references section of this document.

- *The e-safety policy will be available on the school Website.*
- *A partnership approach with parents will be encouraged. This could include offering parent evenings, demonstrations, practical sessions and suggestions for safe Internet use at home.*
- *Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.*
- *Internet issues will be handled sensitively to inform parents without undue alarm.*
- *Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.*
- *Interested parents will be referred to organisations such as PIN, Parents Online and NCH Action for Children (URLs in reference section).*
- *All parents will receive support information as and when available, e.g. Know It All for Parents.*
-

4.4. How will complaints be handled?

Parents and teachers must know how and where to report incidents- see APPENDIX 2. Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the Internet use was within or outside school. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's behaviour policy. All record of the incident should be kept, e.g. e-mails saved or printed, text messages saved etc. Complaints of a child protection nature must be dealt with in accordance with the LA Child Protection procedures.

- *Responsibility for handling incidents will be delegated to a senior member of staff.*
- *Any complaint about staff misuse must be referred to the headteacher.*
- *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 the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.*

Implementing E-Safety at Marlborough St Mary's Primary School

Role	Responsibilities
Governors	• Approve and review the E-safety Policy and Code of Conduct (AUP) • Regular monitoring of E-safety and report to Governors • Ensure the school's internet provision is filtered by SWGFL
Head teacher and Senior Leaders:	• Ensure that all staff receive suitable CPD to carry out their E-safety roles • Ensure that there is a system in place for monitoring E-safety • Follow correct procedures in the event of an E-safety allegation being made • Ensure that the school infrastructure / network is safe and secure and that approved policies and procedures are implemented
E-Safety Leader:	• Ensure all staff are aware of the procedures outlined in the E-safety policy • Provide and / or broker training and advice for staff • Attend updates and liaise with the LA E-safety staff and technical staff • Report to the Senior Leadership Team and Governors on E-safety • Ensure that there is a structured teaching programme for E-safety in place • Ensure there is explicit procedures on the use of personal and mobile devices
Curriculum Leaders	• Ensure E-safety is reflected in teaching programmes where appropriate E.g. PSHME Anti bullying, English copyright, Humanities online research…
Teaching and Support Staff	• Teaching E Safety is the responsibility of all staff and planning will identify appropriate opportunities • Identify and participate in any training and awareness raising sessions • Have read, understood and signed the staff Code of Conduct • Report any suspected misuse or problem to the E-safety lead • Review risks associated with using existing and new technologies before use
Students/pupils	• Participate in E-safety activities, follow the rules and report any suspected misuse • Understand that the E-safety Policy covers actions out of school that are related to their school • Take responsibility for positively managing their own online presence
Parents and carers	• Ensure that their child / children follow acceptable use rules at home • Discuss E-safety issues with their child / children and monitor their home use of ICT (including mobile phones and games devices) and the internet • Keep up to date with issues through school updates and attendance at events
Technical Support Provider	• Ensure the school's ICT infrastructure is secure and is not open to misuse or malicious attack • Ensure staff and classes may only access the school network through an enforced password protection policy, where passwords are regularly changed • Inform the head teacher of issues relating to the filtering applied by the SWGfL • Keep up to date with E-safety technical information • Ensure use of the network is regularly monitored in order that any misuse can be reported to the E-safety Lead for investigation / action / sanction. • Ensure monitoring software and systems are implemented and updated
Community Users	• Sign and follow the AUP before being provided with access to school systems

APPENDIX 1

Teaching E-Safety

Each year group will teach E-safety through the programme of Hector's world from the website www.thinkuknow.com Lesson plans from this site can accessed and used alongside the lesson plans from the Wiltshire scheme of work. **This is stored on the staff drive in the ICT file and with the ICT subject Leader.**

- *E-Safety is referred to regularly during ICT lessons and will also be taught discreetly.*
- *E-Safety posters/displays will be visible in each class and on the laptop trolley.*
- *E-Safety reminders will be attached to the children's computers in the school.*
- *The whole school will promote E-Safety through safer internet day in February each year. http://www.saferinternet.org.uk/safer-internet-day*

Hector's World work can be supplemented by other approved E-Safety programmes at the teacher's discretion such as:

- *CEOP: www.ceop.gov.uk and www.thinkuknow.co.uk*
- *Childnet International: www.childnet.com*
- *Resources in other languages: www.saferinternet.org*
- *Cyberbullying Guidance for teachers and professionals:http://www.digizen.org.uk/downloads/cyberbullying_teachers.pdf*
- *www.teachtoday.eu – excellent site for supporting teachers (and parents with a range of issues)*
- *Key Stage 1 - Hector's World http://www.thinkuknow.co.uk/5_7 - useful for parents to work with children*
- *Who's your friend on the internet? http://www.netsmartzkids.org/activities/whofriend.htm*
- *Social Networking: http://www.kidsmart.org.uk/socialnetworking/*
- *http://www.chatdanger.com/*
- *Validity and Bias: www.allaboutexplorers.com*
- *www.thedogisland.com*
- *The SMART Crew: http://www.childnet.com/kia/primary/*
- *Wild Web Woods – Children's rights etc. www.wildwebwoods.org*
- *Cyberbullying: http://www.digizen.org.uk/cyberbullying/film.aspx*
- *Interactive game: http://www.digizen.org.uk/cyberbullying/film.aspx#interactive*
- *Netsmartz – real lifestories: http://www.netsmartz.org/netteens.htm*
- *NSTeens – cartoons etc. http://www.nsteens.org/*
- *Cyberbmentors – www.cybermentors.org.uk*

Resources that may be useful for parents

- *www.childnet.com/kia/parents - Childnet's Know it All for Parents resource CD – available in 10 languages.*
- *http://www.thinkuknow.co.uk/parents - CEOP's website – aimed at parents including videos and a webcast.*
- *http://www.swgfl.org.uk/Staying-Safe/e-Safety-Movies - Good video clips that are useful to promote parent's evenings*
- *http://www.childnet-int.org/safety/parents.aspx - this includes a downloadable parent presentation*
- *http://www.sgfl.org.uk/E-safety/responsibilities/parents - a range of materials - useful in preparing a presentation*
- *http://www.ofcom.org.uk/research/stats/ - lots of statistics around internet use etc.*

Resources to signpost parents to

- *http://www.parentlineplus.org.uk/index.php?id=246 - DCSF's parentlineplus website -useful hints and tips*
- *http://www.direct.gov.uk/en/Parents/Yourchildshealthandsafety/Internetsafety/index.htm - Useful guidance*
- *http://www.childnet-int.org/downloads/chatGuide.pdf - useful guide for parents about chat*
- *http://www.childnet-int.org/downloads/searchGuide.pdf - A parent's guide to search and search providers*
- *http://cms.lgfl.net/web/lgfl/safety/resources - this LGfL site signposts a range of useful resources for parents, including parent leaflets in 10 languages. There is also a useful esafety leaflet for parents*
- *www.kented.org.uk/ngfl/ict/safety.htm - Kent's resources for esafety which include support leaflets for parents of children and young people.*
- *http://www.rbksch.org/esafety/parent-es.htm - a good list of resources at the bottom of the page.*
- *http://www1.orange.co.uk/safety - safety site from Orange – excellent resources*
- *http://parents.vodafone.com – new website from Vodafone – good content/videos – take the test is a good one*
- ***Digital Parenting Magazine** - http://bit.ly/aWhS4d*

Ref: Wiltshire Council Schools Internet Policy 2013

APPENDIX 2

Responding to incidents of misuse

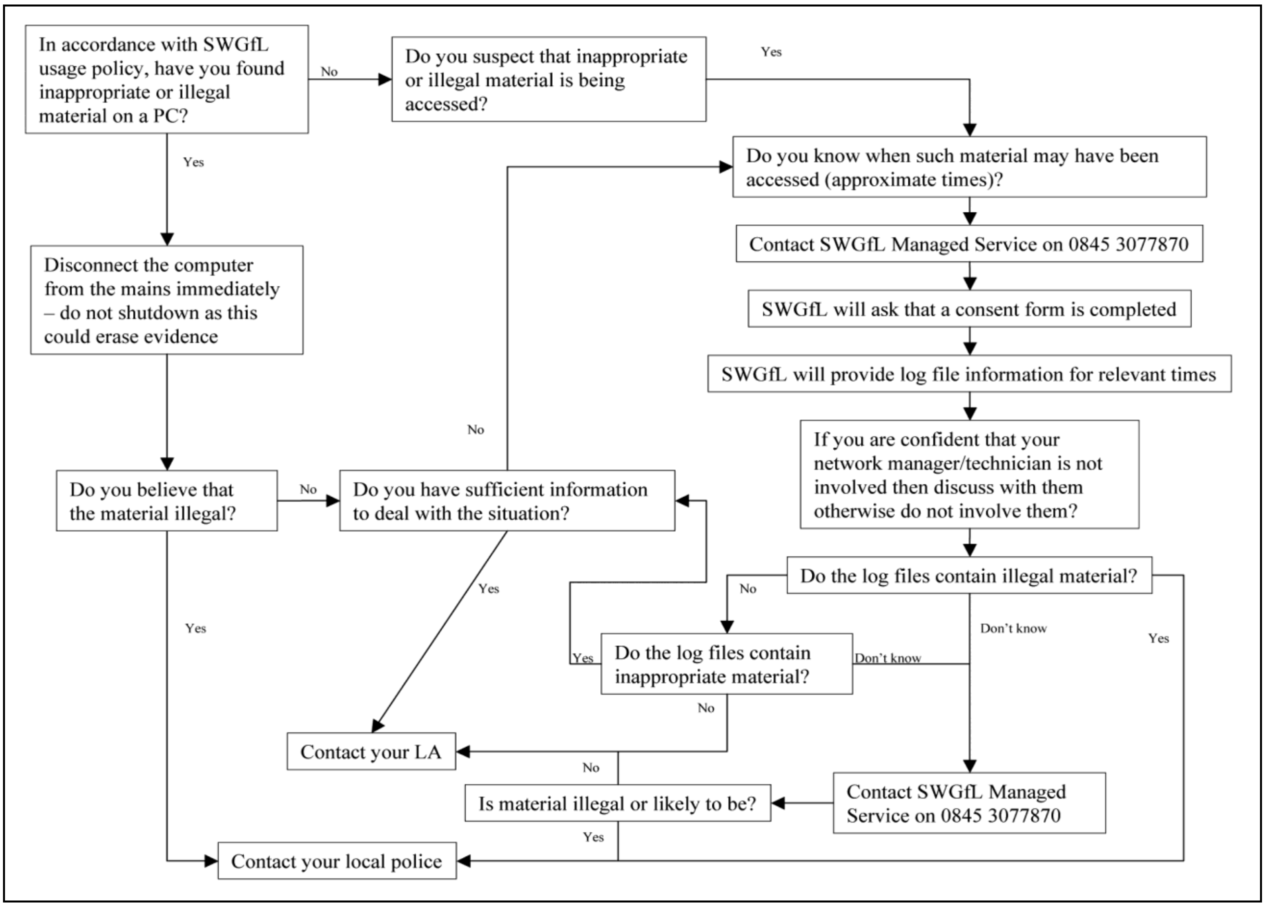
We expect all members of the school community to be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy take place, through careless, irresponsible or, very rarely, deliberate misuse. If any apparent or actual misuse appears to involve illegal activity it is recommended that the SWGfL flow chart below is consulted and followed, in particular the sections on reporting the incident to the police and the preservation of evidence. Illegal activity would include:

child sexual abuse images

adult material which potentially breaches the Obscene Publications Act

criminally racist material

other criminal conduct, activity or materials


In accordance with SWGfL usage policy, have you found inappropriate or illegal material on a PC?
No
Do you suspect that inappropriate or illegal material is being accessed?
Yes
Do you know when such material may have been accessed (approximate times)?
Yes
Contact SWGfL Managed Service on 0845 3077870
Disconnect the computer from the mains immediately – do not shutdown as this could erase evidence
SWGfL will ask that a consent form is completed
SWGfL will provide log file information for relevant times
No
If you are confident that your network manager/technician is not involved then discuss with them otherwise do not involve them?
Do you believe that the material illegal?
No
Do you have sufficient information to deal with the situation?
Do the log files contain illegal material?
Yes
No
Yes
Don't know
Yes
Yes
Do the log files contain inappropriate material?
Don't know
No
Contact your LA
No
Is material illegal or likely to be?
Contact SWGfL Managed Service on 0845 3077870
Yes
Contact your local police

If members of staff suspect that any misuse might have taken place it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event it is suggested that the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" will be followed. This guidance recommends that more than one member of staff is involved in the investigation. 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.

www.swgfl.org.uk/Staying-Safe/Files/Documents/esp_esafety_policy_template

For further help and advice the UK Safer Internet Centre helpline for professionals who work with children and young people in the UK, specifically tackles the area of e-safety.

http://www.saferinternet.org.uk/helpline