Online Safety Policy

ST MARY'S SCHOOL

YATE

Date Agreed: September 2021

Review Date: September 2022

Our vision, Enjoy, Explore, Excel; be amazing is rooted in Psalm 139, which recognises that God made us all in an amazing and wonderful way. We are unique and will fulfil our own potential.

As a school, our 12 Christian Values: responsibility, respect, perseverance, courage, hope, compassion, trust, forgiveness, truthfulness, thankfulness, friendship and peace are interwoven through our curriculum, our interactions and how support the children in making choices in their behaviour. There may be times when the use of force is appropriate and through adherence this policy, we aim to act in a way that is aligned with our values

Online Safety Policy

This Online safety policy has been developed, and will be reviewed and monitored, by our school online safety working group which comprises of:

- ICT Subject Leader
- Headteacher
- A representative of teaching staff and support staff
- A governor representative and a parent representative

Consultation with the whole school community has taken place through a staff meeting, Student Council meeting, governors meeting, parents evening and the school website / newsletter.

Schedule for Monitoring and Review

Policy ratified by the *Governing Body on::*	December 2021
The implementation of this policy will be monitored by:	Online safety working group
Monitoring will take place:	Annually during Term 6 – July 2022
The *Governing Body* will receive a report on the implementation including reported incidents:	Annually during Term 6 – July 2022
This policy will be reviewed:	Annually during Term 1 – September 2022
Should serious Online safety incidents take place, the following external persons / agencies will be informed:	Nick Pearce – Technical and Filtering Jo Briscombe – Teaching and Learning Adviser ICT

Monitoring

The school will monitor the impact of the policy through an analysis of:

- Logs of reported incidents and responses using MyConcern
- Monitoring logs of internet activity and any network monitoring data

- Surveys / questionnaires of students, parents / carers, and staff including non-teaching staff
- Monitoring information about the teaching programme and coverage within the curriculum
- Regularly checking that pupils and staff are clear about how to report incidents and respond to them
- The content of the website, twitter account and Class Dojo is regularly monitored by governors and senior leaders to ensure that it complies with this policy, the acceptable use agreements and user actions/sanctions agreement (Apendixes A-D).
- Any other web site, such as the school friends, that is linked to the school name is also regularly monitored to ensure that the school is always presented accurately and professionally.

Scope of the Policy

This policy applies to **all** members of the school community (including volunteers, parents/carers, visitors and community users) who have access to or use school ICT systems inside and outside school. The Education and Inspections Act 2006 empowers Headteachers, 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 relevant to incidents, including cyber-bullying, which may take place out of school, but are 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, inform parents / carers of known incidents of inappropriate online safety behaviour that take place out of school. The 2011 Education Act increased these powers with regard to searching for and of electronic devices and the deletion of data and related action can only be taken over issues covered by the school behaviour policy. Our behaviour policy states that, when dealing with online safety issues, electronic devices will only be searched and data deleted with parents. If parents are unavailable, the device will be kept securely until a parent can meet to conduct such a search with a senior leader.

This policy should be read alongside the acceptable use policies for staff and pupils, the anti-bullying policy and the behaviour policy.

Roles and Responsibilities

- The governors have overall responsibility for ratifying the policy, ensuring that it is implemented and monitoring it. This action is delegated to the Headteacher.
- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety is delegated to the online safety Leader. The Headteacher is also the designated person for child protection and is trained in online safety issues and aware of the potential for serious child protection issues to arise from sharing of personal data, access to illegal / inappropriate materials, inappropriate on-line contact with adults / strangers, potential or actual incidents of grooming and cyber-bullying.

Training and Awareness Raising

There is a planned programme of Online safety training for **all** staff and governors to ensure that they understand their responsibilities, as outlined in this, and the acceptable use policies. The following actions are undertaken to raise awareness:

- An audit of the Online safety training is carried out annually.
- The Child Protection and Online Safety Leader receive regular updates through attendance at relevant training such as SWGfL and LA training sessions and by receiving regular Online safety updates from the South Gloucestershire Traded Services.

- All staff, including support staff, receive an annual Online safety update.
- Any reported incidents and how they are addressed are discussed at staff meetings and used as an opportunity to test our processes and update staff on how to deal with issues.
- The Online safety Leader provides advice/guidance and training as required to individuals and seeks LA advice on issues where appropriate.
- A training log is used to record when updates and training are delivered.

Induction Processes

- All new staff, parents and children are introduced to the acceptable use policy and the user action/sanction agreement (Appendix A-D)
- Parents of children who join school mid-year are made aware of the processes and their children are also introduced to the acceptable use policy.

Teaching and Learning

Online safety is now a statutory part of the programme of study for all key stages. Rules and technical solutions are are not infallible and we are aware that outside school children will be using unfiltered internet provision. We believe it is crucial to educate children about how to behave responsibly online and how to keep themselves and others safe. Children and young people need the help and support of the school and parents to recognise and avoid online safety risks. There is a planned and progressive scheme of work for online safety, which is taught at every year group. This is based around the South Gloucestershire scheme of work and Digital Literacy Curriculum by SWGfL and, across the key stages, covers:

- Internet safety
- Privacy and security
- Relationships and communication
- Cyberbullying
- Information literacy
- Self-image and identity
- Digital footprint and reputation
- Creative credit and copyright

The scheme of work is delivered as part of computing, PSHE and other lessons.

Regular opportunities will be taken to reinforce online safety messages in all lessons and to teach pupils to be critically aware and consider the accuracy of the information they access online. Online safety messages will also reinforced through other subjects and through a planned programme of other activities such as assemblies and events. Older pupils are taught to acknowledge the source of information and respect copyright. Pupils are helped to understand the AUP, recognise online safety risks, adopt safe practices, report any issues and keep evidence to support reporting (for older children). Staff model safe practice in use of technologies and mobile devices and guide students to appropriate sites and follow practices for dealing with unsuitable material found in internet searches. Where pupils undertake searching of the internet, staff monitor the content of the websites they are visiting. If they identify pupils who may be vulnerable, for example, who are not adopting safe practices or completing inappropriate searches this should be logged and appropriate support given to those pupils to help them understand the risks and what to do to keep safe.

If there are educational reasons why a blocked site is needed for learning then staff can request that this be made available to technical staff. Where this is done this a clearly logged with reasons given for this access.

Children new to the school will be provided with an overview of expectations when they start.

The following aspects also contribute to our curriculum provision:

- Coverage of learning experiences is recorded and staff check understanding when teaching about online safety.
- Annual online safety events such as Safer Internet Day will also used to raise awareness.

Rules for Keeping Safe

These are reinforced through the following:

- Pupils sign an acceptable use agreement and this is also communicated to parents, in Foundation Stage, who we hope will reinforce the messages at home.
- Pupils are helped to understand the student acceptable use policy and school rules for online safety and encouraged to act accordingly.
- All classes have online safety rules displayed in their classroom and staff regularly refer to these, for example, during activities where children are searching the internet for information. Rules are also displayed in other areas where ICT is used.
- Staff act as good role models in their own use of ICT.
- All staff have undertaken awareness training and know that some children are more vulnerable than others to being approached online. Their level of awareness will be tested through regular training. Online behaviour is dealt with in accordance with our behaviour policy. There are sanctions and rewards in place for this.

Education – parents / carers and the community

Parents and carers have an essential role in educating their children and monitoring their behaviour online, however they may have a limited understanding of the risks and issues and underestimate the dangers or be unsure how to deal with them. The school aims to raise awareness and support parents through:

- Curriculum activities
- Letters and newsletters including information on any online safety issues that have been raised in school (anonymously recorded) and how to address these
- Parents / carers information evenings
- Events such as Safer Internet Day
- Providing information and web links about where to access support on the website
- Tweet and Class Dojo information

Parents of children new to the school will be provided with an overview of expectations linked to relevant policies including online safety when their child starts school.

The website also provides information that is relevant for the wider community including grandparents, early years settings and voluntary groups.

Education – staff and volunteers

All staff receive annual online safety training so that they understand the risks and their responsibilities. This includes:

- A planned programme of online safety training, which is regularly updated and reinforced and linked to the expectations outlined in this policy, Keeping Children Safe in Education and in the Ofsted framework.
- An audit of online safety training needs of staff is carried out annually.
- All new staff receive online safety training and training on relevant policies and expectations as part of their induction programme.
- The online safety lead receives regular updates and external training to support them to do their role.
- Policies relevant to online safety and their updates will be discussed in staff meetings.
- The online safety lead provides regular guidance and training to support individuals where required.

Training – governors

Governors take part in online safety training and awareness raising sessions, particularly those governors who are involved with technology and safeguarding. This is offered through:

- Attendance at local authority or regional events
- Attendance at relevant staff training
- Regular newsletter information and access to website information

Self-evaluation and Improvement

The school undertakes self-evaluation in order to inform actions to continually improve online safety provision through the following:

- Local authority safeguarding audit
- 360 degree safe online self-evaluation tool which is also used to benchmark our provision against other schools.
- Surveys with pupils, staff and parents

Technical Issues

The local authority provides technical and curriculum guidance for Online safety issues for **all** South Gloucestershire schools as well as providing direct technical support to a large number of schools.

Password Access to Systems

All our systems are accessed via an individual log in. Users have passwords that include upper and lower case and a number and are encouraged to change these regularly. **Users are told that passwords must never be shared for any IT system and that they are responsible for any actions taking using their log in**. The same log in is used to access our governor online area, computing scheme of work and learner area. Access to systems is through groups so that only the relevant group of users can access a resource.

Internet Provider and Filtering

The South Gloucestershire school internet service is provided by Integra and this includes a filtering service to limit access to unacceptable material for all users.

Internet access is filtered for all users by South Gloucestershire School IT. Illegal content (child sexual abuse images) is filtered by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. However, we are aware that no filtering is completely infallible and consequently focus on teaching pupils to keep safe through our curriculum and teaching. There are two different levels of filtering, which are targeted towards different user groups. As a consequence, teacher and staff users have access to some resources for teaching that are filtered for learners so as to ensure that “over blocking” does not restrict teaching.

Technical staff monitor internet traffic and report any issues to schools.

The school reports issues through logging a call to the service desk at 3838.

Any filtering requests for change and issues are also reported immediately to the South Gloucestershire technical team on 3838. Requests from staff for sites to be removed from the filtered list must be approved by the Headteacher and this is logged and documented by a process that is agreed by the Headteacher.

Technical Staff - Roles and Responsibilities

Where the local authority provides technical support the “administrator” passwords for the school are not held by the school and the local authority are responsible for their security and any implications of their use.

The school ensures, when working with our technical support provider that the following guidelines are adhered to.

- There are regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling are securely located and physical access is restricted.
- All users have clearly defined access rights to school ICT systems and are provided with a username and password by the technical support provider.
- Users are responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Temporary access is provided for “guests” (e.g. trainee teachers, visitors, supply staff) through the use of a handbook, which is received in the morning and returned at the end of the day onto the school system.
- 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 Agreement and user actions/sanctions agreement (Apendixes A-D).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual workstations are protected by up to date virus software.

- The staff/pupil user agreement indicates that the schools forbids staff from installing programs on school and/or portable workstations. This also forbids the use of memory sticks or devices.

Use of Digital Images and Video

Ease of access to technologies which take digital images and video has many benefits for learning. Taking and sharing images and video are much easier and, if not managed, this could increase the potential risk of misuse and has the potential to be used for cyberbullying. The school informs and educates users about the risks associated with digital images and these are outlined in the acceptable use agreement.

- When using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including publishing their own images on social networking sites.
- Pupils should not take, use, share, publish or distribute images / video of others without their permission and staff reinforce this when appropriate.
- Written permission is obtained from parents or carers before photographs of pupils are taken. These photographs are only taken to be used for educational purposes or to promote achievements or the school.
- Staff are allowed to take digital / video images to support educational aims, but follow guidance concerning the sharing, distribution and publication of those images.
- Staff sign permission forms to say that they allow their image to be used for promoting the school and are aware of the risks of this being copied
- Images are only taken and used of individuals where there is a signed permission form in place.
- Pupils full names are not published on any online platform or school communication including the website, newsletter, twitter feed or Class Dojo. Photographs published anywhere that include pupils are carefully selected and not used in association with pupils' full names or other information that could identify them.
- Care is always taken to ensure that pupils are appropriately dressed if images are taken and that they are not participating in any activity, which might bring individuals or the school into disrepute.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use as this is not covered by the General Data Protection Regulation. However, in order to protect other children and respect privacy these images should not be published or made publicly available on social networking sites. Parents / carers should also not comment on any activities involving other pupils in the digital / video images. This is clearly detailed in our acceptable use agreement for parents.
- Pupils' work is only published with the permission of pupils and parents / carers.

Mobile Technologies

These might include mobile phones, tablets or any other device that has the capability of accessing the school's wireless network. The primary use of these in school is to support learning, teaching and management.

Only Senior members of staff (Head teacher and Deputy Head) gain access to wifi on personal devices through the school wifi network.

Children are not allowed to use their personal devices in school as the school provides access to the technologies to be used for learning.

Staff are not allowed to use their personal mobile phones in school while they are teaching and any use should be restricted to times when children are not present. The only exception to this is in case of emergency during a school trip.

Staff do not use their own mobile phone to take images of children, for example, on a school trip as the school has devices available for this.

Communications Technologies and Social Media

A wide range of communications technologies have the potential to enhance learning and management. The acceptable use agreements outline how these systems should be used.

- The official school email service is used for communications between staff, and with parents/carers and students as it provides an effective audit trail. Communications are always professional in tone and content.
- Users are made aware that email communications may be monitored and what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature through the acceptable use policies.
- Governor communications take place through governor school e-mail accounts. Personal or sensitive information is not e-mailed but is kept on a secure online site that governors can access to via a personal user account.
- Personal email addresses, text messaging, public chat and social networking programmes are not be used for communications with parents/carers and children.
- The school uses Twitter / Class Dojo / Texts / Email to update parents on news and events and this is managed and monitored by a named member of staff who approves content and monitors use of the account.
- Personal information is also not posted on the school website and only the office email address is listed for members of staff. The web site is the responsibility of all staff.
- Guidance on personal use of social media and mobile devices is included in the staff, parent and pupil acceptable use agreement, including clear reporting mechanisms. Training is provided for staff and risks, reporting and issues around social networking forms part of the learning for pupils.
- Staff ensure that no reference is made in social media to pupils, parents or other staff and do not engage in online discussions on personal matters about any member of the school community
- Personal opinions are not attributed to the school
- Security settings on personal social media profiles promoted to the staff and encouraged to monitor individually
- Staff personal use of social media where it does not relate to the school is outside the scope of the policy but is should be made clear that the member of staff is not communicating on behalf of the school. If staff come across communications that might bring the school into disrepute in their personal communications they should not get involved, refer the publisher to relevant complaints procedures and report the issue.
- The online safety lead pro-actively monitors the Internet for postings about the school.
- The school also purchase BOOST which includes a reputation alert to support this monitoring.

Copyright

Frankie Oakley is responsible for making sure that software licence audit is regularly updated and also making regular checks to ensure the number of software installations matches the licences held. Where there are insufficient licences this could breach the Copyright Act, which may lead to fines or unexpected additional license costs.

Data Protection

Personal Data is defined as any data which relate to a living individual who can be identified from the data. This includes opinion about the individual. Sensitive Personal Data about a person includes information about their racial or ethnic origin, political opinions, their religious beliefs or other beliefs of a similar nature, whether they are a member of a trade union and their physical or mental health or condition.

Personal data is recorded, processed, transferred and made available according to the General Data Protection Regulation and is:

- 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 and only transferred to others with adequate protection

Transfer of Data

Whenever possible secure online storage is used to ensure that documents do not need to be transferred to limit the risk. We ensure that data is stored in accordance with the requirements laid down by the Information Commissioner’s Office and within the EU. This also applies to cloud storage used.

The school ensures that:

- It holds the minimum personal data necessary to enable it to perform its function and does not hold it for longer than necessary for the purposes it was collected for.
- The data held is accurate, up to date and inaccuracies are corrected as quickly as possible.
- All personal data is fairly obtained in accordance with our “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing” as outlined in the policy on the South Gloucestershire IMS Traded Services web site.
- Personal and sensitive data relating to pupils or staff is not e-mailed as this is not secure.
- Personal data including assessment data is transferred using secure file transfer. .
- It has clear and understood arrangements for the security, storage and transfer of personal data
- It is registered as a Data Controller for the purposes of the General Data Protection Regulation (GDPR)
- There is a Senior Information Risk Officer (SIRO) and Information Asset Owner (IAOs) in place.
- Risk assessments are regularly carried out.
- Data subjects have a right to access their data and there are clear procedures for this.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.

- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- The Data Protection policy highlights the data protection measures that staff should take and how data can be securely stored and deleted.

Staff ensure that they

- Take care to ensure safe keeping of personal data and minimise the risk or loss or misuse
- Use personal data only on secure password protected computers and devices and log off at the end of every session

Reporting and Recording

There are clear reporting mechanisms in place for online safety incidents and all staff are regularly reminded of these and fully aware of their responsibilities to follow up any reported issues.

Online safety issues are reported to the Child Protection Lead. If these include allegations of bullying then the anti-bullying policy is followed. Issues which may impact on the well-being and safety of a child are reported directly to the Child Protection Lead and Child Protection procedures are followed. Issues impacting on staff or to the detriment of the school should be reported to the headteacher or to the Chair of Governors if the headteacher is absent or the accusation involves the headteacher.

Pupils are encouraged to report any incidents to an adult whether it relates to themselves or a friend. We encourage children to take responsibility for protecting each other.

Managing Incidents (See Appendix C)

In the event of suspicion of an infringement of policy then all the following steps should happen.

- More than one senior member of staff should be involved in investigating to protect possible future accusations.
- Use a computer that will not be used by young people which could be taken off site by the police if required.
- Ensure staff have internet access to investigate but that sites and content are closely monitored and recorded.
- Record the URL of any site containing alleged misuse and the nature of the content causing concern. It may be useful to record and store screenshots of the content by printing them, signing them and attaching them to the record. Except for child abuse images as this would constitute an offence.
- Once the investigation is complete the investigating group should identify the appropriate response in line with policies which may internal procedures, involvement of LA or police.

Reporting to the police

- If the content being reviewed includes images of child abuse then monitoring should be stopped and the police informed immediately. Other incidents to be referred to the police are
    - incidents of ‘grooming’ behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials

  In any of the above isolate the computer involved as any change to its stage may hamper a police investigation.

If issues could be a result of problems with infrastructure or may affect it then the technical support provider is informed immediately (for South Gloucestershire support 3838).

If access to an unsuitable site is reported then the Online Safety lead will alert the technical support team by ringing 3838 to ensure that this is blocked. Serious incidents are escalated to local authority staff for advice and guidance

Nick Pearce – infrastructure, technical and filtering – 01454 86**3838**

Jo Briscombe – curriculum and policy – 01454 86**3349**

Tina Wilson – LADO allegations against staff and volunteers – 01454 86**8508**

Access and response team (ART) – safeguarding / child protection concerns **-** 01454 86**6000** (Monday to Friday) and 01454 615165 (Out of hours/Weekends)

For incidents affecting school staff the Professionals Online Safety Helpline is contacted for advice if necessary on helpline@saferinternet.org.uk or 0844 381 4772.

Communication Technologies **Appendix A**	Allowed		Allowed at certain times		Allowed for selected staff	Allowed with staff permission	Not allowed	
	Staff	Pupils	Staff	Pupils	Staff	Pupils	Staff	Pupils
Mobile phones may be brought to school			√			√		
Use of mobile phones in lessons							√	√
Use of mobile phones in social time	√							√
Taking photos on mobile phones or other camera devices			√			√		
Use of hand held devices eg PDAs, PSPs			√					√
Use of personal email addresses in school, or on school network	√							√
Use of school email for personal emails							√	√
Use of chat rooms / facilities							√	√
Use of instant messaging							√	√
Use of social networking sites			√					√
Use of blogs	√					√		

User Actions (Appendix B)

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

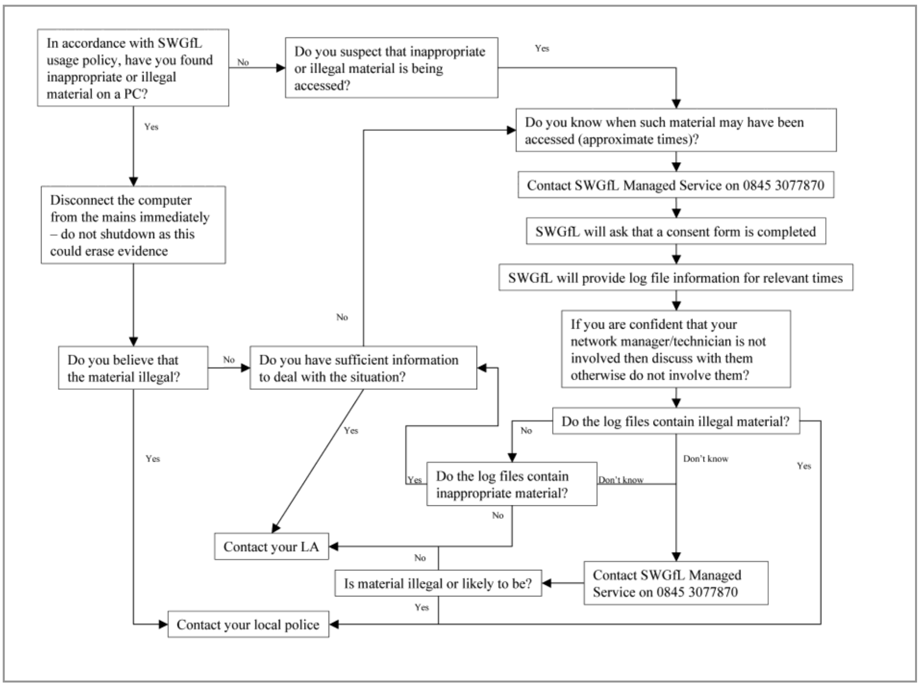
Responding to incidents of misuse (Appendix C)

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 ie.

- 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.


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
Yes
Do you know when such material may have been accessed (approximate times)?
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 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 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 (Appendix D)

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	√	√	/	/	/	/	/	√	

Staff Incident (Appendix E)

Incidents:	Refer to line managerr	Refer to Headteacher	RRefer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		√	√	√				√
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		√	√					√