Robert Le Kyng Primary School E-Safety Policy

Background / Rationale

New technologies have become integral to the lives of children and young people 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. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

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 include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- 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
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Illegal downloading of music or video files

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 (eg. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, 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.

This school recognises its duty to protect our students from indoctrination into any form of extreme ideology which may lead to the harm of self or others. This is particularly important because of the open access to electronic information through the internet. The schools aims to safeguard young people through educating them on the appropriate use of social media and the dangers of downloading and sharing inappropriate material which is illegal under the Counter-Terrorism Act.

We provide the children and parents with opportunities and training to develop the necessary skills to manage and reduce these risks. The e-safety policy that follows explains how we to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Monitoring

The school will monitor the impact of the policy using:

- Logs of incidents
- Staff feedback through staff meetings and meetings with computing/E-Safety leaders
- Pupil voice (school council)
- Outcomes of "staying safe" questionnaire
- Monitoring of planning and lesson evaluations through normal school cycle

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, 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 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 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.

Roles and Responsibilities

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

Governors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The Headteacher will report any incidents that are entered into the e-safety log and the CP governor will review e-safety as part of the annual Child Protection audit and mid-year review.

Headteacher and Senior Leaders:

- The Headteacher 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 Leaders.
- The Headteacher and members of the Senior Leadership Team are responsible for ensuring that the E-Safety Leaders 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 Headteacher 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 Headteacher and another member of the Senior Leadership Team 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 Appendix 1)

E-safety Leaders

In this school the leadership of e-safety is carried out jointly by the Computing subject leader and the Designated Safeguarding Lead who:

- take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provide training and advice for staff
- liaise with the Local Authority
- liaise with school ICT technical staff
- receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments
- attend relevant meeting / committee of Governors
- report regularly to Senior Leadership Team, when the Headteacher will take on the investigation of the incident with support from co-ordinator and e-safety governor

Network Manager/Technical staff

The ICT Technician 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 Local Authority E-Safety Policy and guidance (SWGfL Security Policy – Appendix 4)
- 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
- that he / she keeps 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 E-Safety Co-ordinator for investigation / action / sanction

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They DO NOT have pupils as friends on social networks such as Facebook.
- they have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the E-Safety Leaders / Headteacher, as soon as possible, for investigation / action / sanction
- digital communications with pupils (Email / Voice /text –Mobiles etc) should ONLY be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use 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

- 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

Designated Safeguarding Lead

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

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

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.

- 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, i-pads and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. 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 e-safety sessions, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy
- accessing the school website / VLE / future on-line pupil records in accordance with the relevant school Acceptable Use Policy

Community Users

Community Users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign a Staff/Volunteer AUP before being provided with access to school systems.

Policy Statements

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 will be provided as part of the computing curriculum and PHSE and should be regularly revisited – this will cover both the use of computers and new technologies in school and outside school
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and class sessions to be provided by ICT co-ordinator / Headteacher / Class teachers
- 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

Education – Parents/carers
Many parents and carers have an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. 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.
"There is a generational digital divide". (Byron Report).
The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, school website
- Parent training sessions
- Reference to the SWGfL Safe website (the SWGfL "Golden Rules" for parents)

Education and 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.
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies (this is included in their online Child Protection training package)
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Leaders (or other nominated person) will provide advice / guidance / training as required to individuals as required

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / SWGfL or other relevant organisation.

- Participation in school training / information sessions for staff or parents

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 Network Manager (or other person) and will be reviewed, annually, by the E-Safety Committee (or other group).
- All adult users will be provided with a username and password by the ICT Technician who will keep an up to date record of users and their usernames. Pupil access will be through individual logons but with restricted access to some aspects of the network.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher with the Headteacher having logon rights to this system.
- Users will be made 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.
- The school maintains and supports the managed filtering service provided by SWGfL
- Any filtering issues should be reported immediately to SWGfL through the ICT Technical support system.
- Requests from staff for sites to be removed from the filtered list will be considered by the HEADTEACHER in consultation with the E-safety co-coordinators. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Network Technician
- 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.
- 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.
- All staff who require it, will be given an encrypted data storage device so that data is not left vulnerable in public places
- The school infrastructure and individual workstations are protected by up to date virus software.

Curriculum
E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of computing 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, eg 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 that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- 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.

Use of digital photographic and video images

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. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate 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 eg. on social networking sites.
- 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. Those images should be taken on school equipment but the personal equipment of staff may be used for such purposes. These images are to be moved to the school system immediately and removed from the device.
- Care should be taken when taking digital / video images that students / 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.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Parents/ carers will have an opt out option for the use of digital video/ photographs of their children for educational purposes.

Data Protection

The school must ensure that:

- It has a Data Protection Policy.
- It has appointed a Data Protection Officer (DPO).
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

Staff must ensure that they

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school / academy policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X						x	
Use of mobile phones in lessons			x					x
Use of mobile phones in social time	x							x
Taking photos on mobile phones or other camera devices		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 educational 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.
- 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, chat, VLE 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.
- Staff must not communicate with children (under the age of 18) that they have come into contact with through their professional position, using electronic communication devices or social networking sites. Staff who have contact with pupils and ex-pupils through personal relationships should, if possible, declare the issue to an E-safety leader and ensure that if any issues arise that the E-safety leader is informed immediately.
- 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.

Unsuitable / Inappropriate 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.

The school policy restricts certain internet usage as follows:

User Actions		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**					X
	promotion or conduct of illegal acts, eg 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 (eg 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 eg Youtube		X				
Communicating in an electronic form with ex pupils under the age of 18					X	

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 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 – (appendix 1) and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Pupils

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).		X	X	X					
Unauthorised use of non-educational sites during lessons	X				x				
Unauthorised use of mobile phone / digital camera / other handheld device	X					X			
Unauthorised use of social networking / instant messaging / personal email	x				X	X			
Unauthorised downloading or uploading of files	X				x	X			
Allowing others to access school network by sharing username and passwords	x				X	X	X		
Corrupting or destroying the data of other users	x		x			X			
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	x		x			X			
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x		x			X			
Deliberately accessing or trying to access offensive or pornographic material	x		x		x	x	X		

Staff

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X			X
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	X	X				X		
Careless use of personal data eg holding or transferring data in an insecure manner		X				X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X						X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X				X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X				X		
Actions which could compromise the staff member's professional standing		X				X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X				X		X
Using non-approved proxy sites or other means to subvert the school's filtering system		X				X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident		X			X			
Deliberately accessing or trying to access offensive or pornographic material		X					X	X
Inappropriate electronic contact (communications or through social networking sites) with children that are known in a professional basis		X						X

Date on which policy was approved: Nov 2018

Policy review date: Nov 2020

Appendix 1
Allegation Procedures

1. Incident to be logged with the E-safety co-ordinator and on the logging system on the network.

2. Incident to be investigated by E-safety co-ordinator/ SMT/ Headteacher.

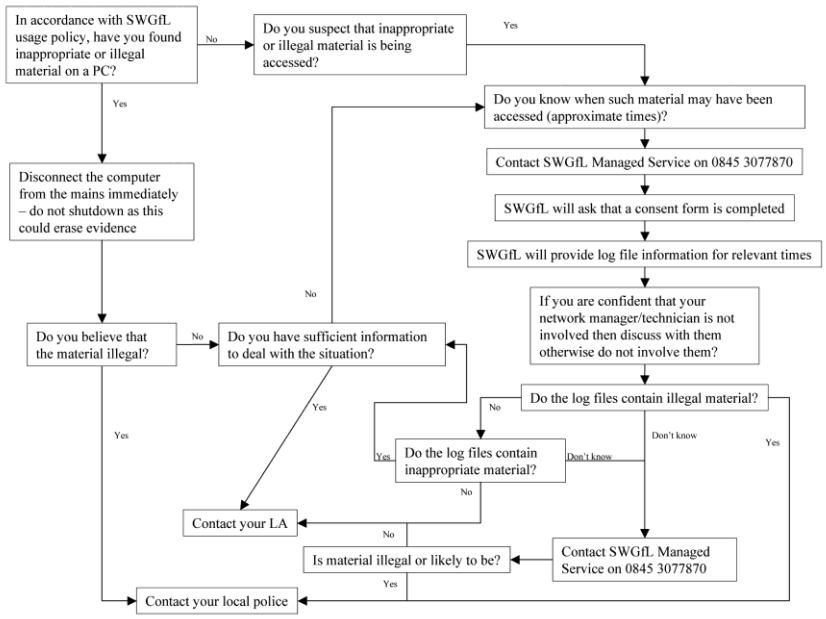
3. Report to be produced by E-Safety Co-ordinator.

4. Sanctions to be decided (see sanctions list in main body text).

5. Report of incident to E-Safety Governor.

6. For serious child safety/ illegal incidents Swindon LA E-Safety Officer to be informed and other relevant agencies to be involved (Police and Social Services).

SWGFL Allegation Flow Chart



Appendix 2
Reportage of safety incidents

Incidents that occur (such breach of filtering or misuse of ICT resources within school) should be reported to the Headteacher ensuring that the following information is available. There is a log of incidents kept in a locked drawer in the headteacher's office.

This will ask for nature of the incident, time and date, if possible, of the incident, pupils/ staff involved.

- Nature of Incident
- Date of incident
- Time of incident
- Individuals involved
- Action Taken

Appendix 3
Portable and Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Portable & Mobile ICT Equipment

This section covers such items as laptops, PDAs and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on School systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is backed up appropriately (preferably on the school network)
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the ICT support team.
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

SWGfL **Security Policy**

The security policy applied to the South West Grid for Learning (SWGfL) covers the following areas and protocols:

- Schools will be able to access Web sites on the Internet through Proxy Servers sited in the Core. Direct access to Internet Web sites from stations inside the SWGfL is not allowed
- Schools will be able to have access to the standard RM news services. Access to other news services on the Internet is denied
- The stations on the school's LAN will be able to talk to DNS servers in the Core. This will allow DNS name resolution for all sites inside the SWGfL and the Internet
- Stations and servers on the Internet will be able to browse to Web sites hosted on the Virtual Web Servers (VWS) sited in the Core. Schools within the SWGfL will be able to upload Web sites to the VWS
- Video conferencing using the H323 protocol is only enabled through the SWGfL Gatekeeper. Sites can configure their settings on the Gatekeeper to control sites (internal and external) to which they can video conference. Also, importantly, schools that choose to have a local firewall or proxy may not be able to utilise the video conferencing service or may be limited to one designated video conference enabled station inside the LAN
- SMTP Mail Relay Servers at the Core will handle mail between the Internet and the SMTP mail servers on the schools' LANs inside the SWGfL
- If required schools can synchronise their computer's time with a designated time server at the Core
- Management and backup of the Core servers are permitted from designated management stations at IFL (Internet For Learning).
- RM SafetyNet™ updates are allowed from the RM SafetyNet server to the Core sited SafetyNet Proxy Servers
- All other traffic between establishments inside or outside the Grid will be blocked

The table overleaf outlines the technical configuration of the central firewall service.

Security Configuration

The general principles of this security policy are as follows:

- No traffic shall enter or leave the SWGfL Infrastructure without being explicitly permitted by the firewall
- No traffic shall route directly between connected establishments unless having been explicitly allowed to do so

From	To	Protocol/Port	Action	Log	Comment
Rules to allow any required connections to the firewall from the FireWall Management Server Rules to allow any required connections to the FireWall Management Server, such as management traffic from RM Drop everything else trying to connect to the firewall (stealth rule) & log					
Connected Establishments	WAN Centre Proxy/DNS Servers/VWS	HTTP8080 / DNS / FTP	Allow	No log	DNS Lookup
WAN centre child proxies	Virus scan proxies	HTTP	Allow	No log	Referral to parent proxy
Virus scan proxies	Internet	HTTP	Allow	No log	'Dirty' HTTP requests
WAN Centre Proxy/DNS Servers	The Internet	HTTP / HTTPS FTP / DNS	Allow	No log	Outbound proxy access to the Internet
Connected Establishments	WAN Centre News proxy	NNTP	Allow	No log	News (virus scan proxies as news proxies)
RM News server	WAN Centre News proxy	NNTP	Disallow	No Log	News feed. WAN Centre news server acting as news proxy. Only allowed on explicit request
Internet	WAN Centre VWS/DNS	HTTP / DNS	Allow	No Log	Inbound HTTP for VWS
Connected Establishments	Internet	(H323)	Disallow	No Log	
Internet	Connected Establishments	(H323)	Disallow	No Log	
VC stations at sites (no Local firewall)	VC stations at sites (no local firewall)	(H323)	Allow	No Log	
Connected Establishments	VC stations at sites (with a local firewall)	(H323)	Allow	No Log	Restricted to one identified station at the site with the local firewall
VC stations at Connected Establishments (with a local firewall)	Connected Establishments	(H323)	Allow	No Log	Restricted to one identified station at the site with the local firewall
Connected Establishments	SWGfL SMTP Mail Relay Servers	SMTP	Allow	No Log	Outbound SMTP
Any Host	SWGfL SMTP Mail Relay Servers	SMTP	Allow	No Log	Inbound SMTP
Connected Establishments	SWGfL Mail Servers	POP3	Allow	No Log	Inbound POP3
Connected Establishments	WAN Centre time server	NTP	Allow	No Log	Time service to Connected Establishments
194.238.49.0/24	All WAN Centre equipment except fw-1 and fwmng	telnet / pcAnywhere pcAnywhere data pcAnywhere stat	Allow	short	IFL management connections to WAN Centre
Each WAN Centre subnet (not including.32/27)	Backup	Legato Ports	Allow	short	Rules to allow backup between subnets in WAN Centre
RM SafetyNet update server	WAN Centre Proxy Servers	331 SQL database update	Allow	No Log	SafetyNet Updates

Drop everything else and log (deny all rule). One Security policy applied to all sites

South West Grid *for* **Learning**, Great Moor House, Bittern Road, Sowton, Exeter EX2 7NL
Tel: **01392 381371** Fax: **01392 381370** Email: **enquiries@swgfl.org.uk** Web site: **www.swgfl.org.uk**

PN 3302 11/05