THE ACORNS PRIMARY and NURSERY and WHITLEY VILLAGE FEDERATED SCHOOL

E-SAFETY POLICY

March 2017

Acknowledgment. SWGfl (http://www.swgfl.org.uk/) has been used as the source for this policy.

INTRODUCTION

Communication with Children *(including the Use of Technology)*

Communication between children and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.

Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. E-mail or text communications between an adult and a child/young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites.

Internal e-mail systems should only be used in accordance with the organisation's policy.

This School E-Safety Policy has been developed to consider all current and relevant issues, in a whole school context, linking with other relevant policies, such as the Safeguarding policy.

National guidance suggests that it is essential for schools to take a leading role in e-safety. Becta[1] in its "Safeguarding Children in a Digital World" suggested:

> *"That schools support parents in understanding the issues and risks associated with children's use of digital technologies. Furthermore, Becta recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for e-safety within the school. Recognising the growing trend for home-school links and extended school activities, Becta recommends that schools take an active role in providing information and guidance for parents on promoting e-safety messages in home use of ICT, too."*

Footnote: *Becta was the government agency leading the national drive to ensure the effective and innovative use of technology throughout learning. It was established in 1997, and was closed on 31 March 2011. The Department for Education (DfE) continues key areas of Becta's work.*

The Byron Review "Safer Children in a Digital World" stressed the role of schools:

> *"One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."*

The development and expansion of the use of Computing, and particularly of the internet, has transformed learning in schools in recent years. 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 pupils at risk within and outside the school.

Children and young people will need to develop high level Computing skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that Computing can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks."

However, schools must, through their e-safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. This policy will also form part of the school's protection from legal challenge, relating to the use of ICT.
The School is expected to evaluate its level of e-safety in the Ofsted Self Evaluation Form (SEF) in readiness for an increased level of scrutiny by Ofsted Inspectors during school inspections.

SCOPE

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

RESPONSIBILITIES

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the School Improvement Committee and the full Governing body receiving regular information about e-safety incidents and monitoring reports. The Governor Responsible for Safeguarding is also the governor responsible for e-safety (this must be a separate appointment to the Computing Link Governor). The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator Lead Teacher
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

Headteacher and Senior Leaders:

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community.

The Headteacher is responsible for ensuring that the 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 Leadership Team will receive regular monitoring reports from the Headteacher.

The Headteacher and another member of staff 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 "Responding to incidents of misuse")

Appointed e-Safety Co-ordinator

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to the Headteacher

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

- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- 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.

The Local Authority Network Manager 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 Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- the school's filtering policy (through Securus), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- 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/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the E-Safety Co-ordinator for investigation
- that monitoring software/systems are implemented and updated as agreed in school policies

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 have read, understood and signed the school Staff Acceptable Use Policy
- they report any suspected misuse or problem to the E-Safety Co-ordinator for investigation
- digital communications with pupils (email/Virtual Learning Environment/ voice) should 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, extra-curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

The Safeguarding Officer

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

(It is important to emphasise that these are child protection/safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop.)

Pupils:

- are responsible for using the school ICT systems in accordance with the Acceptable Use Policy, which they will be expected to sign before being given access to school systems. (Note: at KS1 it would be expected that parents/carers would sign on behalf of the pupils)
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyberbullying.
- 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' evenings, newsletters, letters, website/virtual learning environment and information about national/local e-safety campaigns/literature.

Parents and carers will be responsible for:

- endorsing (by signature) the Acceptable Use Policy
- accessing the school website/virtual learning environment in accordance with the Acceptable Use Policy.

The acceptable use policy and further advice on the application of sanctions is set out in the Appendix 1,2, 3 & 4.

Guidance for Publishing Content

The school website is an excellent medium for communicating with families both current and prospective as it can celebrate pupils' work, promote the school and publish resources for projects. However, publication of information should be considered from a personal and school security viewpoint.

§ The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published, e.g. photographs of pupils will never be named.

§ The Executive head teacher will take overall editorial responsibility along with the Mrs Lesley McLaren, ICT Technician and Computing link Governor and ensure that content is accurate and appropriate.

Can pupil's images or work be published?

Still and moving images and sounds add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount.

§ Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified (i.e. never named).

§ Pupils' full names will not be used anywhere on the website, particularly in association with photographs, where no names will be used.

§ Written permission from parents or carers will be obtained before images of pupils are electronically published in any format.

How will social networking and personal publishing be managed?

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control.

For use by responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published.

Examples include: blogs, wikis, Twitter, Bebo, Pinterest, Facebook, Windows Live Spaces, MSN space, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

- The schools firewall will block or filter access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be taught not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.

- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for student use on a personal basis.
- Students should be advised not to publish specific and detailed private thoughts.
- Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

ACCESS TO INAPPROPRIATE SITES

It is not acceptable to use any equipment in the workplace in any of the following contexts:

- Illegal activity.
- Activities for private gain.
- Personal shopping.
- Excessive personal messages.
- Playing games.*
- Gambling.
- Political comment or any campaigning.
- Personal communications to the media.
- Use of words or visual images that are offensive, distasteful or sexually explicit.
- Insulting, offensive malicious or defamatory messages or behaviour.
- Harassment or bullying.
- Random searching of the web.
- Accessing sites which could be regarded as sexually explicit pornographic or otherwise distasteful or offensive.
- Using message encryption or anonymised web search, except where encryption is required for official ***school/***Council business purposes.
- Racist, sexist or other conduct or messages which contravene the Council's employment diversity policies.
- Actions which could embarrass the school/Council or bring it into disrepute.

See Appendix 5 for a detailed list of equipment and activities consider appropriate/inappropriate for staff and pupils.

INADVERTENT ACCESS TO INAPPROPRIATE SITES AND INAPPROPRIATE EMAILS

If an employee inadvertently accesses an inappropriate web site, they should leave it immediately but notify their school of the incident, giving the date and time, web address (or general description) of site and the action taken. This will help safeguard their position in circumstances where disciplinary action would otherwise result.

Employees may find themselves receiving emails which contravene this policy. In the case of comparatively innocuous material (e.g. 'clean jokes'), the recipient should point out to the sender that they do not wish to receive such messages at their workplace because they believe they contravene the school's/Council's policy. If there is repetition, the employee should retain the messages and notify their Headteacher. If the emails are racist or sexist or could otherwise be regarded as offensive, they should be left in the inbox and the Headteacher notified immediately. Employees should notify the sender that they do not wish to receive further such material and keep a record of doing so.

Appendix 1

Acceptable Use of Technology
Code of Conduct

Introduction

ICT in its many forms – internet, email, mobile devices etc – are now part of our daily lives. It is our duty to ensure that they are used safely and responsibly. All staff at The Acorns and Whitley Village Federated School are aware of the following responsibilities:

- All staff, Governors and visitors understand that ICT includes a wide range of systems, including mobile phones, digital cameras, laptops and tablets.

- All staff, Governors and visitors understand that it is a disciplinary offence to use the school ICT equipment for any purpose not permitted by its owner. Please refer to the acceptable use policies for further information.

- No staff, Governors or visitors will disclose any passwords provided to them by the school.

- All staff, Governors and visitors understand that they are responsible for all activity carried out under their username.

- Staff, Governors and visitors will not install any hardware or software on any school owned device without the Head's permission.

- All staff, Governors and visitors understand that their use of the internet is monitored and if anything untoward is uncovered, could be logged and used in line with any disciplinary procedures. This includes all school owned devices, even when used off the school premises. If an e-safety incident should occur, staff will report it to the designated lead for safeguarding as soon as possible.

- All staff, Governors and visitors will only use the school's email / internet / intranet etc and any related technologies for uses permitted by the Head or Governing Body. If anyone is unsure about an intended use, they should speak to the Head beforehand.

- All staff, Governors and visitors will ensure that data is kept secure and is used appropriately as authorised by the Head or Governing Body. No passwords should be divulged and only encrypted memory sticks should be used.

- Personal devices must only be used in the context of school business with the explicit permission of the Head. Personal mobile phones or digital cameras must not be used for taking any photographs related to school business. Each class has access to a tablet or digital camera specifically for this purpose. These devices must never be used for personal use.

- All staff, Governors and visitors using school equipment will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- All staff, Governors and visitors will only use the approved email system for school business.

- Images will only be taken, stored and used for purposes within school unless there is parental permission for alternative use. Our parents/carers are asked to sign if they agree to their children's images being used for school advertising, publishing on the website/Twitter feed or in the local press. If a parent/carer does not agree to this, we ensure that their child's photograph is not used.

- All staff, Governors and visitors will make every effort to comply with copyright and intellectual property rights.

- All staff, Governors and visitors will report any incidents of concern regarding staff use of technology and/or children's safety to the Head or the Deputy safeguarding leader in line with our school's Safeguarding Policy.

I acknowledge that I have received a copy of the Acceptable Use of Technology Code of Conduct.

Full Name ____

Signature ____

Date __________________

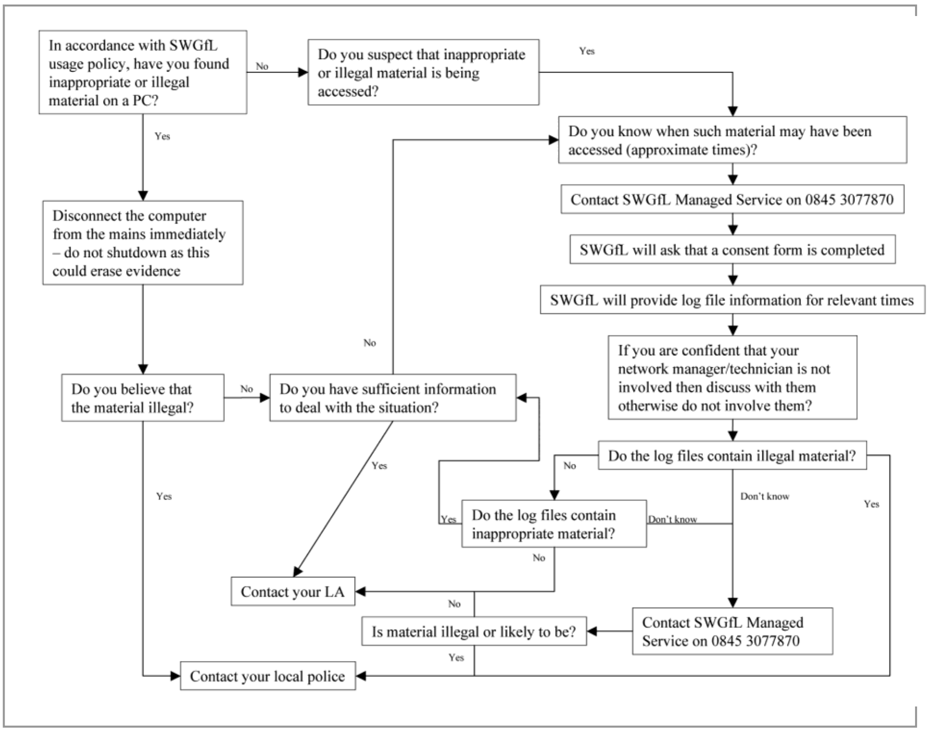
Appendix 2

RESPONDING TO INCIDENTS OF MISUSE

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:
If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The flow chart – below 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
Do you know when such material may have been accessed (approximate times)?
Contact SWGfL Managed Service on 0845 3077870
SWGfL will ask that a consent form is completed
SWGfL will provide log file information for relevant times
If you are confident that your network manager/technician is not involved then discuss with them otherwise do not involve them?
Do the log files contain illegal material?
Yes
Disconnect the computer from the mains immediately – do not shutdown as this could erase evidence
No
Do you believe that the material illegal?
No
Do you have sufficient information to deal with the situation?
Yes
Yes
No
Do the log files contain inappropriate material?
Yes
Don't know
Don't know
Yes
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 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 using the pro-formas given on the SWGfL website.

Appendix 3

SANCTIONS FOR E-SAFETY AND CYBERBULLYING INCIDENTS

It is the policy of the school to use any e-safety incidents as a Teaching & Learning opportunity. Sanctions are only used at the Headteacher's and class teacher's discretion and in conjunction with T & L.

Regardless of having the best e-safety policies and practice in place, there may still be occasions when e-safety/cyberbullying incidents occur. The two AUP policies (for adults and children) outline appropriate and inappropriate behaviours and sanctions for misuse, and this document also contains clear guidelines for responding to e-safety incidents, and clear lines of communication for escalating specific incidents where necessary. Everyone must be aware of the process. Escalation of incidents may take place within the school or other service setting, or may require the notification and disclosure to external agencies such as the LSCB, the police or another appropriate agency. The school considers various e-safety scenarios, responses and reporting mechanisms – for example: Accidental or deliberate access to inappropriate material

The definition of 'inappropriate' may change according to your users or the setting. The AUP makes clear what is deemed to be inappropriate material within various contexts, and the sanctions which will apply. Different approaches may be necessary depending on whether the access was accidental or deliberate.

Accidental or deliberate access to illegal material
If filters are correctly set, it should not be possible to access illegal materials. Settings should be checked on a regular basis to ensure that they filter as expected, and the levels of filtering are appropriate for the end-user. If illegal material is accessed, escalation of the incident will be necessary.

Inappropriate use of email or other technologies
Again, the definition of inappropriate may change according to your users or the setting. The AUP makes clear what is deemed to be inappropriate use of email and other technologies within various contexts, and the sanctions which will apply.

Illegal use of email and other technologies
Illegal use of email and other technologies should always be escalated to an appropriate agency.

Deliberate misuse of the network (for example, hacking, virus propagation or circumventing safety controls).
The AUP clearly states what is deemed to be inappropriate use of network resources, the monitoring that is in place and the sanctions which will apply to deliberate misuse. If networks have been used for illegal activity, the incident should be escalated accordingly.

- Accidental or deliberate access to inappropriate material
- Accidental or deliberate access to illegal material
- Inappropriate use of email or other technologies
- Illegal use of email and other technologies
- Deliberate misuse of the network 45 AUPs in context: Establishing safe and responsible online behaviours

Bullying or harassment using technologies
Bullying or harassment is not acceptable in any circumstance, via any means, and responses should mirror those documented in established anti-bullying policies. It may also be necessary to involve appropriate external agencies, depending on the severity of the event.

Sexual exploitation using technologies
This is a serious offence, and will require escalation to appropriate external agencies as necessary. Depending on the nature of the event, different e-safety incidents will require different responses, and undoubtedly no two e-safety incidents will be exactly the same. This does not mean, however, that responses should be left to chance and circumstance: instead the school attempts to model general processes and procedures for responding to incidents as appropriate to your context, drawing on good practice within the wider field of child protection. Such exercises can often be effective as both awareness raising and training tools. Incidents may involve children and young people, staff, or others as both victims and perpetrators, and the school's response model must be capable of dealing with each of these quickly and effectively.

Appendix 4

EXAMPLES OF RESPONSE PROCEDURES TO E-SAFETY INCIDENTS.

The following matrix offers examples of typical incidents and suggestions as to possible responses. The School's Behaviour Policy, indicates what sanctions are applied.

Child as Victim				
Hazard	**Examples**	**Prevention**	**Proposed Response**	**Comments**
Receiving unsolicited content that is inappropriate, obscene, offensive or threatening	Web sites (often through mis-clicked or mis-typed web addresses); email (Spam); banner advertising; pop-ups (largely eradicated through better browser design).	Educator vigilance; Acceptable internet Use Policy known by all users, and is enforced by school. Effective web filtering in place. Using safe filtered email. Effective spam filtering. Maintain email and URL logs and history.	Complete a risk assessment to determine severity of impact on the child. As the content is unsolicited, there can be no question of culpability of the child. Follow-up to prevent recurrence, including ensuring that relevant sites are blocked if required. Inform parents where appropriate. Ensure incidents are reported and recorded.	*Protective measures are essential; however it is not acceptable to be so risk averse that access is removed entirely. Procedures are agreed with parents and Governors for reporting abuse.*

Child as Victim				
Hazard	**Examples**	**Prevention**	**Proposed Response**	**Comments**
Child is the subject of published material.	Images stored in publicly accessible areas; Personal blogs such as MSN spaces, BEBO etc.; Details left on web sites. Incitement: hatred and discrimination, personal harm etc.	Educator vigilance; Acceptable internet Use Policy known by all users, and children made aware of the dangers.	Complete a risk assessment to determine the severity of impact on the child. Determine if a perpetrator / victim relationship may exist. Where an in-school perpetrator is identified, and a crime has taken place, police should be informed. Disciplinary action may follow. Where an external perpetrator is identified, report to police. Follow-up to prevent recurrence, including ensuring that relevant sites are blocked if required. Inform parents where appropriate.	*Most image storage sites have levels of access, usually private; family & friends and public. These sites are great fun for sharing images; however care should be taken, as users may be able to access inappropriate images posted by others.*

Child as Victim				
Hazard	**Examples**	**Prevention**	**Proposed Response**	**Comments**

Bullying and Threats	Email; text messaging;
	blogs; sexting; selfharm sites, drug
	forums; suicide sites;
	hate sites;
	Instant Messenger.
	Incitement: hatred and discrimination, personal harm etc.
		Reinforcement of school ethos and behaviour.
		Regular sample trawls of known sites. Anti-bullying initiatives should accompany efforts to promote internet use
			Complete a risk assessment to determine the severity of impact on the child.
			Determine if a perpetrator / victim relationship exists.
			Where a perpetrator is identified take appropriate disciplinary action.
			Follow-up to prevent recurrence, including ensuring that relevant sites are blocked if required.
			Inform parents where appropriate.
			Online and offline bullying should be seen as connected.
			Although children have a range of coping mechanisms, support is needed for the victim to ensure as often they do not tell a trusted adult or friend.
			The bully themselves may be vulnerable so appropriate counselling will also be needed.
			Raising awareness for teachers, parents and Children about the array of risks that keep changing on the Internet
				There is no real difference between bullying and threats using technology and more familiar means. Bullying and threatening behaviour is damaging and wrong and should be treated very seriously.

Child as Victim				
Hazard	**Examples**	**Prevention**	**Proposed Response**	**Comments**
Security	Adware; browser hijack; virus.	Secure and up to date browser settings and antivirus software; regular adware scans.	Effective reactive technical intervention.	*This is a frequent problem that is amplified where operating systems and browsers are not regularly updated. It can often occur where inappropriate sites have been visited.*

Child as Victim				
Hazard	**Examples**	**Prevention**	**Proposed Response**	**Comments**
Predation and grooming	Forming online relationships by deception with the intent of gaining the confidence of a minor to do harm.	Teach awareness of dangers. Use the 'Think U Know' teaching resources.	Where a perpetrator is identified, take appropriate disciplinary/legal action and in the first instance refer to police. Follow-up to prevent recurrence, including ensuring that relevant sites are blocked if required. Early advice to parents with regard to computer and games console locations, use and mobile technology.	*Grooming and predation is a child protection issue and should be reported to the Designated Safeguarding Lead, social care or police in all cases, or referred to the CEOP through their reporting web site.*

Child as Victim				
Hazard	**Examples**	**Prevention**	**Proposed Response**	**Comments**
Requests for personal information, financial cheating	‘Phishing' is the use of deceit to obtain personal (usually financial) information.	Teach awareness of dangers.	If identity theft occurs it should be reported to police without exception.	*Most 'phishing' is aimed at adults with banking facilities, so older children are more likely to be affected.*

Child as Instigator				
Hazard	**Examples**	**Prevention**	**Proposed Response**	**Comments**
Soliciting content that is inappropriate, obscene, or offensive.	Use of inappropriate search terms; Accessing or forwarding the details of known sites; Following inappropriate links or banners; inappropriate image searches.	Use safe image search engines. Effective web filtering. Educator vigilance. Effective incident reporting procedures for blocking sites once known.	Inform parents using a letter. Restrict computer or internet access for a fixed period, dependent on severity. Maintain incident records to identity patterns of behaviour. If a crime has taken place, report it to the police i.e. making /distributing images or communications offences	*Maintain records of incidents to identify serial offenders.*

Child as Instigator				
Hazard	**Examples**	**Prevention**	**Proposed Response**	**Comments**
Sends or publishes content that is inappropriate, obscene, offensive or threatening.	Emails; blogs; msn-spaces; social networking sites; and chat rooms.	Block access to specific sites.	Maintain records of incidents to identify regular offenders. Inform parents using a standard letter. Remove computer access for a fixed period. If a crime has taken place, report it to the police i.e. making /distributing images or communications offences	*The medium is less important than intent. Publishing is easy using the web; however in legal terms it can still be libellous and subject to the same legal remedies. Where there are known sites that do not moderate effectively they should be blocked.*

Child as Instigator				
Hazard	**Examples**	**Prevention**	**Proposed Response**	**Comments**
Identity Theft, personal information abuse.	Using others identity to gain access to school systems or services.	Systematic changes of password. Alternative methods of authentication, such as swipe card or fingerprint.	Recover identity and change password. Inform parents using a standard letter. Restrict computer or internet access for a fixed period, dependent on severity. Follow up to prevent recurrence, including ensuring that relevant sites are blocked if required.	*It is essential that schools consider carefully where personal data is stored, and who can access this data. Access to names and addresses must be secure, and DBS (CRB) checks in place to protect children.*

Appendix 5

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					/
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					/
	adult material that potentially breaches the Obscene Publications Act in the UK					/
	criminally racist material in UK					/
	pornography				/	
	promotion of any kind of discrimination				/	
	promotion of racial or religious hatred				/	
	threatening behaviour, including promotion of physical violence or mental harm				/	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				/	
Using school systems to run a private business					/	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					/	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					/	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					/	
Creating or propagating computer viruses or other harmful files					/	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					/	
On-line gaming (educational)		/				
On-line gaming (non educational)					/	
On-line gambling					/	
On-line shopping / commerce			/*			
File sharing					/	
Use of social networking sites					/	
Use of video broadcasting eg Youtube				/^		

* Only if the shopping is for products necessary for school

^ Only for watching videos. Only if deemed educational beneficial and a member of teaching staff accesses it.

POLICY REVIEW

The Governing Body of our school is responsible for ensuring the review of this policy.

Approved by the Full Governing Body:

Review Date:

Signed:

Chair of Governors