2015-2016

E-Safety/Online 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 students/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 requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, families, members of the community and the young people themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil/student 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
- Risk of being groomed by those whom they contact on the internet.
- The sharing/distribution of personal images without consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- Inability to evaluate the quality, accuracy and relevance of information on the internet

- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- Potential for excessive use which may impact on the social and emotional development and learning of the young person.

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 students'/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. The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their families) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development/Monitoring/Review of this Policy

This policy has been developed by a working group across the Federation consisting of

- Anne Davies - Finance/SLT
- Lyn Williams - Commissioning
- Maggie Blaber/Stella Taylor – Safeguarding Officers/SLT
- Justin Sharp/Danny Bentham – ICT Managers
- Richard Hunter – ICT Curriculum lead
- Amy Ley – Advocacy/Student Council

Schedule for Development/Monitoring/Review

This e-safety policy was approved by the Governing Body on:	Autumn 2015
The implementation of this e-safety policy will be monitored by the:	E-Safety Group
Monitoring will take place at regular intervals:	Annually
The Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Annually
The E-Safety Policy will be reviewed every three years, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	Autumn 2018
Should serious e-safety incidents take place, the following external persons/agencies should be informed:	Head Teacher, IT Manager, Police, LA Safeguarding Officer

The school will monitor the impact of the policy using:

- Logs of reported incidents
- SWGfL monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys/questionnaires of
  - students
  - Families
  - staff

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, families, 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 students 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 families 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. This will be carried out by the Governing body receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Group
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors meeting

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including online-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Headteacher/Senior Leaders are responsible for ensuring that the E-Safety Coordinator 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/Senior Leaders 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. Such staff will be offered counselling through Wellbeing at Work where appropriate.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.
- 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 online safety allegation being made against a member of staff. (see SWGfL flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR/disciplinary procedures)

E-Safety Coordinator:

- leads the e-safety group
- 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 online safety incident taking place.
- Co-ordinates 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 online safety developments
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meeting
- reports regularly to Senior Leadership Team

Network Manager/Technical staff:

The Network 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
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- SWGfL is informed of issues relating to the filtering applied by the Grid
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that 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
- provides training and advice for staff
- 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/Officer for investigation/action/sanction
- 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/Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator for investigation/action/sanction
- digital communications with students 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
- students/pupils understand and follow the school e-safety and acceptable use policy
- they carefully supervise all 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 students/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
- Students / pupils are not be allowed unsupervised access to the internet

Safeguarding Designated Officer

should be trained in online 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

E-Safety Group

Members of the E-safety group will assist the E-Safety Coordinator with:

- the production/review/monitoring of the school e-safety policy/documents.
- the production/review/monitoring of the school filtering

Students:

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- where appropriate need 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 cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school

Families

Families 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 families 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, website and information about national/local e-safety campaigns/literature.

Community Users

Community Users who access school ICT systems as part of Hollow Lane Club activities will be expected to sign a Community User AUP before being provided with access to school systems.

Policy Statements

Education – students

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

Online Safety education will be provided in the following ways:

- Online Safety should be discussed wherever appropriate when using the internet and as part of lessons. Staff should deliver Online Safety messages at the level the student is able to understand. This will cover both the use of ICT and new technologies in school and outside school
- Key online safety messages should be reinforced as part of assemblies and pastoral activities
- Pupils should be taught to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Pupils should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Rules for use of the internet will be posted in all rooms
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – families

Many families have only a limited understanding of online safety risks and issues, yet they play 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, web site,
- Parents evenings
- Reference to the SWGfL Safe website (nb the SWGfL "Golden Rules" for parents)

Education – Wider Community

The school will offer learning courses in ICT, media literacy and online safety so that parents can gain a better understanding of these issues. Messages to the public around online safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training – Staff

- It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The E-Safety Coordinator will receive regular updates through attendance at SWGfL/LA/other information/training sessions and by reviewing guidance documents released by BECTA/SWGfL/LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in meetings/training events.
- The E-Safety Coordinator will provide advice/guidance/training as required to individuals as required

Training – Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub committee/group involved in ICT/online 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 online safety responsibilities.

- School ICT systems will be managed in ways that ensure that the school meets the online 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
- 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 and will be reviewed, at least annually, by the E-Safety Group.
- All staff/approved persons will be provided with a username and password the Network Manager who will keep an up to date record of users and their usernames. Users will be required to change their password every 6 months.
- The “master/administrator” passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a the school safe
- 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

- The school has provided enhanced user-level filtering through the use of the Impero filtering programme at Ellen Tinkham and ABTutor at Bidwell Brook.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to SWGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and E Safety Co-ordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place for users to report any actual/potential e-safety incident to the Network Manager or E Safety Co-ordinator. This should be advertised through, training, notices and staff newsletters.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, Hollow Lane Club, visitors) onto the school system.
- An agreed policy is in place regarding the downloading of executable files by users (see Staff Acceptable Use Statement)
- An agreed policy is in place regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on laptops and other portable devices that may be used out of school
- An agreed policy is in place that allows staff to install programmes on school workstations/portable devices. Permission must first be sought from the Network Manager. (see Staff Acceptable Use Statement)
- An agreed policy is in place regarding the use of removable media (eg memory sticks/CDs/DVDs) by users on school workstations/portable devices. (see Staff Acceptable Use Statement)
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see Staff Acceptable Use Statement)

Curriculum

Teachers should reinforce online 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.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, and discrimination) 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

Bring your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of online safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of date, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

USE OF DIGITAL AND VIDEO IMAGES - PHOTOGRAPHIC, VIDEO

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. 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 e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, families are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should families comment on any activities involving other students. A declaration not to share images should be signed by families.
- 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 only be taken on school equipment; **the personal equipment of staff should not be used for such purposes.**
- 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.
- Students/pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from families will be obtained before photographs of students are published on the school website (may be covered as part of the AUP signed by families at the start of the year
- Student's work can only be published with the permission of the student and families.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
    - the data must be encrypted and password protected
    - the device must be password protected (many memory sticks/cards and other mobile devices cannot 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 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	✓						✓	
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			✓				✓	

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or families (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.
- Whole class or group email addresses will be used for pupils. Pupils must not be allowed unsupervised access.
- Students 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.

MOBILE PHONES

Staff and visitors should not use their personal mobile phones in the presence of students.

Use of mobile phones on site is only allowed in office areas, meeting rooms and the staff room.

Staff should only use non camera enabled mobile phones to use in an emergency when working with pupils. offsite. The school has purchased several of these and has issued at least one to each class and several more for the Inclusion Team, and Outdoor Education team.

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	✓				

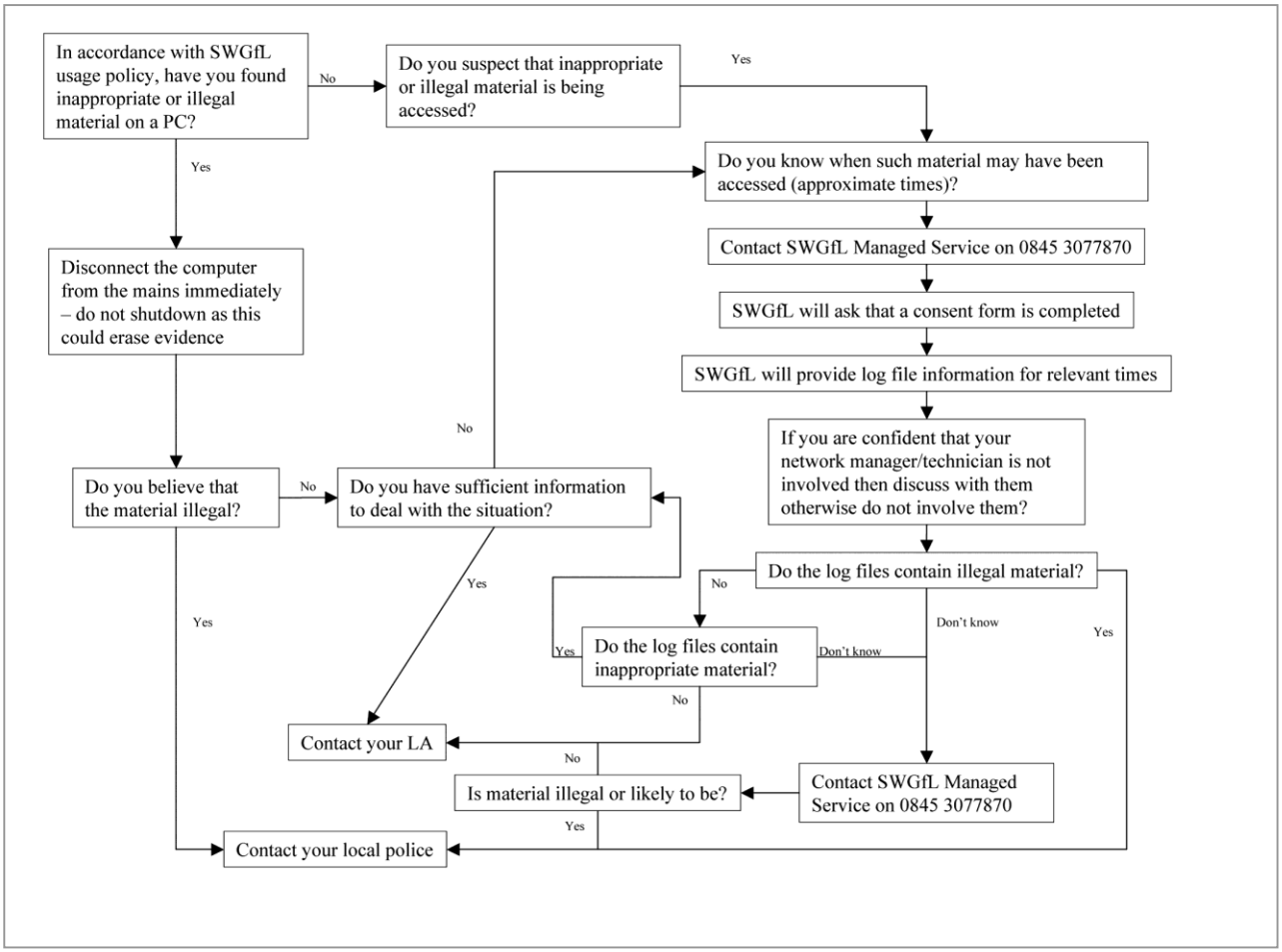
RESPONDING TO INCIDENTS OF MISUSE

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 – below and at 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:

Students/Pupils Actions/Sanctions

Incidents:	Refer to class teacher/tutor	Refer to Head of Department/Head of	Refer to Headteacher	Refer to Police	Refer to technical support staff for action	Inform parents/carers	Removal of network/internet	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	Actions/Sanctions							
Incidents:	Refer to line managerr	Refer to Headteacher	RRefer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action	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		✓			✓			

STAFF INFORMATION SYSTEMS CODE OF CONDUCT

(STAFF ACCEPTABLE USE STATEMENT)

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role at all times.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my use of information systems and the Internet to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I understand that to enhance security my password will need to be changed on a regular basis.
- I will not install any software or hardware without permission from the ICT Technician/Headteacher.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will ensure that any data taken off school premises is stored on an encrypted school USB memory stick or password protected laptop.
- I acknowledge that USB memory sticks are for the secure transportation of work to and from school and that USB memory sticks are not to be used to store information long term.
- I will respect copyright and intellectual property rights, and will liaise with the ICT technician regarding any use of music in lessons, clubs, performances or video recordings.
- I will report any incidents of concern regarding children's safety to the Designated Senior Person for Child Protection/Safeguarding.
- I will report any incidents of concern regarding use of the internet, filtering and E Safety to the Network Manager or E Safety coordinator
- I understand that I am responsible for the appropriate use of any school IT equipment issued to me and for the actions of any others that I allow to use it.

- I understand that I must report any faults with IT equipment issued to me to the Network Manager when they occur and that these items may be recalled on a regular basis for monitoring and updating.
- I will ensure that any electronic communications with pupils or parents/carers are compatible with my professional role.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I will comply with the Devon County Council guidelines that electronically held images should be held in a password protected directory with restricted access and ensure that only authorised access can take place
- I will comply with the Learn to Live Social Media Policy

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or storing unauthorised or unlawful text, imagery or sound.

Staff Agreement Form

I have read, understood and agree with the Information Systems Code of Conduct

Signed ……Print……Date…….

Accepted for school: ……..Print……..

Parent/Carer Acceptable Use Policy Agreement

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

This Acceptable Use Policy is intended to ensure that:

- young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to be responsible users. Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent/Carers Name	
Student Name	

As the parent/carer of the above pupil, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

I know that my son/daughter has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

I understand that the school is not responsible for any material accessed at home or any content found on a personal IPad, Mobile phone or device brought in to school.

Signed _____ Date _____

School Filtering Policy

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.
As a part of the South West Grid for Learning (SWGfL) schools and connected organisations automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Network Manager. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems. To ensure that there is a system of checks and balances and to protect those responsible, changes to the SWGfL/school filtering service must:

- be logged in change control logs
- be reported to the E-Safety Co-ordinator each term in the form of an audit of the change control logs

All users have a responsibility to report immediately to the Network Manager any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Education/Training/Awareness

Pupils will be made aware of the importance of filtering systems through the e-safety education programme. Staff users will be made aware of the filtering systems through:

- signing the AUP
- induction training
- staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through e-safety awareness sessions/newsletter etc.

Changes to the Filtering System

Users may request changes to the filtering system by contacting the Network Manager. Changes will be allowed only if there are strong educational reasons for doing so and The Network Manager will refer the matter to the E-Safety Co-ordinator for approval.

All changes should be reported via the Change Log which will be reviewed by the E Safety Co-ordinator or termly.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Network Manager who will decide whether to make school level changes. If it is felt that the site should be filtered (or unfiltered) at SWGfL level, the Network Manager should email filtering@swgfl.org.uk with the URL.

Monitoring

Ellen Tinkham's filtering system will be monitored using Impero and Bidwell Brook using ABTutor software.

Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the E Safety Co-ordinator
- E-Safety Group
- E-Safety Governors
- SWGfL/Local Authority on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

School Password Security Policy

Introduction

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system

A safe and secure username/password system is essential if the above is to be established and will apply to all school ICT systems.

Responsibilities

The management of the password security policy will be the responsibility of the Network Manager. All users will have responsibility 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.

Users will change their passwords every six months.

Training/Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access/data loss. Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-safety policy and password security policy
- through the Acceptable Use Agreement

Pupils/students will be made aware of the school's password policy:

Policy Statements

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 and will be reviewed, at least annually, by the E-Safety Committee.

All users will be provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames. Users will be required to change their password every term

The following rules apply to the use of passwords:

- passwords must be changed every six months.

- the last three passwords cannot be re-used
- the password should be a minimum of 6 characters long and
- must include two of – uppercase character, lowercase character, number, special character
- the account should be "locked out" following six successive incorrect log-on attempts
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords shall not be displayed on screen, and shall be securely hashed (use of One-way encryption)
- requests for password changes should be authenticated by the ICT Technician to ensure that the new password can only be passed to the genuine user.
- Each user must have their own password. There will be no class logins.

The "master/administrator" passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in the school safe.

Audit/Monitoring/Reporting/Review

The Network Manager will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ons
- Security incidents related to this policy

In the event of a serious security incident:

- the police may request and will be allowed access to passwords used for encryption.
- Local Authority Auditors also have the right of access to passwords for audit investigation purposes

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner. These records will be reviewed by E-Safety Officer at regular intervals. This policy will be regularly reviewed annually in response to changes in guidance and evidence gained from the logs.