Prep School Online Safety Policy

Created: 1st September 2016
Reviewed and updated: September 2018
Date for next review: September 2019
Created by: Director of Studies

A. Introduction

The Internet is now regarded as an essential resource to support teaching and learning.
Young people have access to the Internet from many places, home, school, friends' homes, libraries and mobile phones. Schools have a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use.

Online safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The School's Online Safety Policy should operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

B. Schedule for Development, Monitoring and Review

The implementation of this policy will be monitored by the:	IT Committee
The *Governing Body / Sub Committee* will receive a report on the implementation of this policy including reported incidents:	
This policy will be reviewed regularly and in the light of significant new developments or threats to online safety.	Annually during Term 1
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Sarah Patterson – Head and Safeguarding John Chambers – Network Manager Jane Ellis-Walker – Director of Studies

The school will monitor the impact of the policy using:
- Logs of reported incidents
- SWGfL monitoring logs of internet activity and any network monitoring data from the School technical team
- Surveys / questionnaires of students, parents and staff including non-teaching staff

C. Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors and community users) who have access to and are users of school ICT systems, both in school and out of school where actions relate directly to school set activity or use of school online systems. The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students / 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 such as cyber-bullying, which may take place out of school, but are linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, inform parents / carers of known incidents of inappropriate online safety behaviour that take place out of school.

The following sections outline the roles and responsibilities, policy statements and education in relation to online safety for individuals and groups within the school.

D. Roles and Responsibilities

These are clearly detailed in Appendix 1 for all members of the school community.

The Head is responsible for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety is delegated to the Online Safety Leader. The designated person for child protection is trained in online safety issues and is aware of the potential for serious child protection issues to arise from sharing of personal data, access to illegal / inappropriate materials, inappropriate on-line contact with adults / strangers, potential or actual incidents of grooming and cyber-bullying.

E. Staff and Governors

There is a planned programme of online safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the acceptable use policies.

- An audit of the online safety training needs of all staff is carried out annually.
- All new staff receive online safety training as part of their induction programme
- The Online Safety Leader receives regular by reviewing regular online safety updates from the SWGfL.
- This Online Safety Policy and its updates are shared and discussed in staff meetings.
- The Online Safety Leader provides advice/guidance and training as required to individuals as required.

F. Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of students in online safety is therefore an essential part of our 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.

- There is a planned online safety programme (scheme of work) detailed below.
- Key online safety messages are reinforced annually through an assembly and Online Safety Week.
- Students are helped to understand the student acceptable use policy and act accordingly
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems are posted in all rooms where ICT is used and displayed on log-on screens.
- Staff act as good role models in their own use of ICT.

G. Curriculum

Online safety is a focus in all relevant areas of the curriculum. The online safety scheme of work is linked to the Becta Signposts to safety key online safety elements of culture, contact, commerce and content. It identifies for each year group progression statements, learning outcomes, processes, skills and techniques, vocabulary, suggested software and web links, sample activities and assessment activities.

- In lessons where internet use is pre-planned, students are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches. Staff pre check any searches.
- Where students are allowed to freely search the internet, e.g. using search engines, staff are vigilant in monitoring the content of the websites the young people visit and encourage students to use specific search terms to reduce the likelihood of coming across unsuitable material.

- Students are taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Online safety is covered as part of the Computing curriculum and also incorporated in the PSHE programme.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

H. Parents / Carers

Parents and carers have a critical role to play in supporting their children with managing online safety risks at home, reinforcing key messages about online safety and regulating their home experiences. The school supports parents to do this by:

- Providing clear acceptable use policy guidance and regular newsletter and web site updates
- Inviting parents to attend online safety events.

I. Technical Staff - Roles and Responsibilities

The local authority provides technical guidance for online safety issues, and the team are fully informed about the issues. Where the local authority provides technical support the "administrator" passwords for the school are not held by the school and the local authority are responsible for their security and any implications of their use.

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

- School ICT Systems are 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 relevant Local Authority online safety guidance.
- There are regular reviews and audits of the safety and security of the school's ICT Systems.
- Servers, wireless systems and cabling are securely located and physical access is restricted.
- All users have clearly defined access rights to school ICT systems.
- All users are provided with a username and password by the technical support provider.
- Users are responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by SWGfL.
- Requests from staff for sites to be removed from the filtered list must be approved by the head teacher and this is logged.
- In the event of the school technician needing to make requested changes to filtering, or for any user, this is logged and carried out by a process that is agreed by the Head.
- Any filtering issues are reported immediately to the SWFfL technical team.
- 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.
- Actual / potential online safety incidents are documented and reported immediately to the Online Safety Leader who will arrange for these to be dealt with immediately in accordance with the school's sanction policy.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Guests and visitors are expected to sign the Staff Acceptable Use Policy before being allowed to use ICT systems or devices within the school.
- An agreed policy is in place (Staff and Pupil Acceptable Use Policy) regarding the downloading of executable files by users
- 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. (see School Personal Data Policy Template in the appendix for further detail)

- An agreed policy is in place that allows staff to / forbids staff from installing programmes on school workstations / portable devices (Staff Acceptable Use Policy).
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices. (see School Data Protection Policy)
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet via e-mail or taken off the school site.

J. Use of Digital and Video Images – Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students/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 reported incidents of employers carrying out internet searches for information about potential and existing employees. The school informs and educates users about these risks and implements policies to reduce the likelihood of the potential for harm:

- When using digital images, staff educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.
- Staff ensure that pupils also act in accordance with their acceptable use policy.
- Students' work is only published on a public web site with the permission of the student and parents or carers.

K. Guidance on the Use of Communications Technologies

A wide range of communications technologies have the potential to enhance learning

- The official school email service is used for communications between staff, and with parents/carers and students as it provides an effective audit trail.
- Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Users are made aware that email communications may be monitored and what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature through the acceptable use policies.
- Whole class or group email addresses will be used at KS1, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use only.
- Students / pupils are taught about email safety issues through the scheme of work and implementation of the acceptable use policy.
- Personal information is not sent via e-mail as this is not secure. Personal information is also not posted on the school website and only official email addresses are listed for members of staff.

. The following table shows how the school currently considers these should be used.

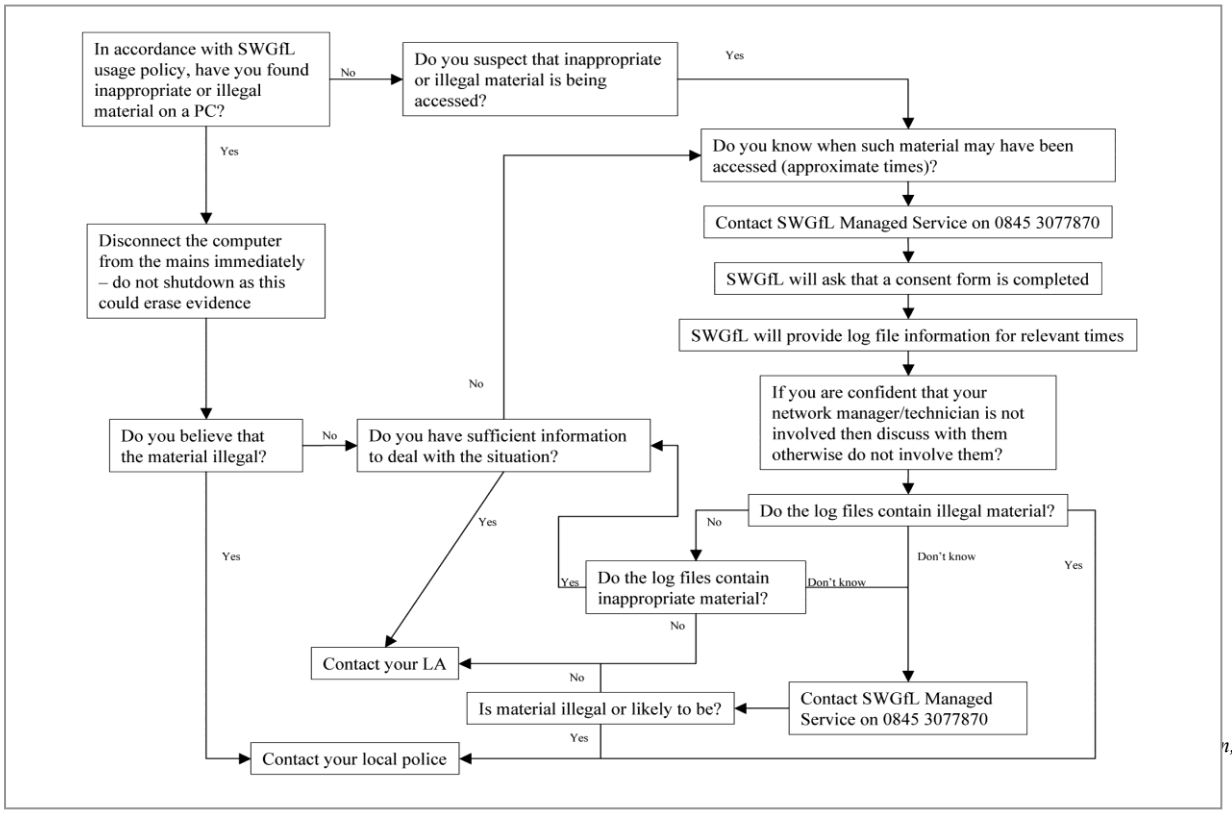
Communication Technologies	Staff & other adults				Students / Pupils			
	Allowed	Allowed at certain times (not during teaching times)	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school		√				√		
Use of mobile phones in lessons				√				√
Use of mobile phones in social time	√							√
Taking photos on mobile phones or other camera devices				√*				√
Use of personal email addresses in school, or on school	√							√
Use of school email for personal emails				√				√
Use of chat rooms / facilities				√				√
Use of instant messaging				√				√
Use of social networking sites				√				√
Use of blogs (school related)		√					√	

** Written permission may be obtained from the Head in the case of exceptional circumstances*

L. Responding to Incidents of Misuse

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

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



n, NW1 5JR.

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

M. Unsuitable/Inappropriate Activities

The school believes that the activities referred to below are inappropriate school and that users should not engage in these activities in school or outside school when using school equipment or systems.

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, e.g. under 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, 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 (e.g. financial / personal, 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 personal shopping / commerce				√		
File sharing of personal information					√	
Use of social networking sites					√	

Use of video broadcasting e.g. YouTube (not school related)				√	

Appendix 1: Roles and Responsibilities

Role	Responsibility
Governors	• Approve and review the effectiveness of the Online Safety Policy and acceptable use policies • Online safety Governor works with the Online Safety Leader to carry out regular monitoring of online safety incident logs, filtering, changes to filtering and then reports to Governors
Head and Senior Leaders:	• Ensure that all staff receive suitable CPD to carry out their online safety roles and sufficient resource is allocated. • Ensure that there is a system in place for monitoring online safety • Follow correct procedure in the event of a serious online safety allegation being made against a member of staff • Inform the local authority about any serious online safety issues including filtering • Ensure that the school infrastructure / network is safe and secure and that policies and procedures approved within this policy are implemented.
Online safety Leader:	• Lead the Online Safety Working Group and dealing with day to day online safety issues • Lead role in establishing / reviewing online safety policies / documents, • Ensure all staff are aware of the procedures outlined in policies • Provide and/or brokering training and advice for staff, • Attend updates and liaising with the LA online safety staff and technical staff, as appropriate • Deal with and log online safety incidents including changes to filtering, • Meet with Online Safety Governor to regularly to discuss incidents and review the log • Report regularly to Senior Leadership Team
Curriculum Leaders	• Ensure online safety is reflected in teaching programmes where relevant e.g. anti-bullying, English publishing and copyright and is reflected in relevant policies.
Teaching and Support Staff	• Participate in any training and awareness raising sessions • Have read, understood and signed the Staff Acceptable Use Agreement (AUP) • Act in accordance with the AUP and Online Safety Policy • Report any suspected misuse or problem to the Online Safety Co-ordinator • Monitor ICT activity in lessons, extra-curricular and extended school activities
Students / pupils	• Participate in online safety activities, follow the acceptable use policy and report any suspected misuse • Understand that the Online Safety Policy covers actions out of school that are related to their membership of the school
Parents and carers	• Endorse (by signature) the Student / Pupil Acceptable Use Policy • Ensure that their child / children follow acceptable use rules at home • Discuss online safety issues with their child / children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet • Access the school website in accordance with the relevant school Acceptable Use Policy. • Keep up to date with issues through school updates and attendance at events
Technical Support Provider	• Ensure the school's ICT infrastructure is secure in accordance with Becta guidelines and is not open to misuse or malicious attack • Ensure users may only access the school network through an enforced password protection policy, where passwords are regularly changed for those who access children's data • Inform the head teacher of issues relating to the filtering applied by the Grid • Keep up to date with online safety technical information and update others as relevant

	• Ensure use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinator for investigation / action / sanction. • Ensure monitoring software / systems are implemented and updated • Ensure all security updates / patches are applied (including up to date anti-virus definitions, windows updates) and that reasonable attempts are made to prevent spyware and malware.
Community Users	• Sign and follow the AUP before being provided with access to school systems.