AMS School Online Safety Policy

Quick Reference

School Online Safety Policy

1. 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 online 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, parents, members of the community and the pupils 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 by using digital devices, being online and through social media include:

- Access to illegal, harmful or inappropriate images or other content.
- Putting themselves at risk through the sharing of images such as sexting.
- Unauthorised access to / loss of / sharing of personal information.
- The risk of being subject to grooming/child sexploitation by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication / contact with others, ncluding strangers.
- Cyber-bullying.
- Access to unsuitable video / internet games.
- Exposure to radicalization and extremism.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The 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 online safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

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 online 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 parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

2.1 Development / Monitoring / Review of this Policy

This online safety policy has been developed by a working group / committee made up of:

- *School Online Safety Champion*
- *Headteacher / Senior Leadership Team (SLT)*
- *Teachers*
- *Support Staff*
- *ICT Technical staff*
- *Governors*

Consultation with the whole school community has taken place through the following:

- *Staff meetings*
- *School / Student / Pupil Council*
- *Governors meeting*

2.2 Schedule for Development / Monitoring / Review

The school Online safety Policy will be reviewed annually.

The school will monitor the impact of the policy using:

- *Logs of reported incidents placed on My Concern and SIMs*
- *SWGfL monitoring logs of internet activity (including sites visited)*
- *Internal monitoring data for network activity*
- *Surveys / questionnaires of pupils (eg Ofsted "Tell-us" survey / CEOP ThinkUknow survey)*
- Parents / carers
- Staff

3. Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, governors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online 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 online safety behaviour that take place out of school.

4. Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

4.1 Governors:

Governors are responsible for the approval of the Online safety Policy and for reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of *Safe Guarding Governor.* The role of the Safe Guarding Governor will include:

- *regular meetings with the Online Safety Champion*
- *regular monitoring of online safety incident logs*
- *reporting to relevant Governors meeting*

4.2 Headteacher , Senior Leaders and Designated Safety Lead (DSL):

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Champion and DSL.
- The Senior Leadership Team (SLT) are responsible for ensuring that the Online Safety Champion and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The SLT will receive termly monitoring reports from the Online Safety Champion.
- The Headteacher and another member of the SLT 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).

4.3 Online Safety Champion:

- Takes day to day responsibility for monitoring online safety issues and has a leading role in establishing and reviewing the school online 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.
- Provides training and advice for staff.
- Liaises with the WAT.
- Liaises with school ICT technical staff..
- Liaises with other outside agencies such as the SWGFL and SSCT.
- Receives reports of online safety incidents via My Concern and reviews onlline incidents to inform future online safety developments.
- Meets regularly with safe guarding lead to discuss current issues, review incident logs and filtering / change control logs.

4.4 Network Manager / Technical staff:

The Network Manager / ICT Co-ordinator 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 online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant latest update of keeping children safe in education.
- That users may only access the school's networks through a properly enforced password protection policy.
- SWGfL is informed of issues relating to the filtering applied by the Grid.

- 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 they keeps up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the / Officer /SLT/DSL/ICT Co-ordinator / Class teacher / Head of Year (as in the section above) for investigation / action / sanction.
- That monitoring software / systems are implemented and updated as agreed in school policies.

4.5 Teaching and Support Staff:

are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices.
- They report any suspected misuse or problems by staff or pupils to the Online Safety Champion/ Officer /SLT/ICT Co-ordinator /DSL/ Class teacher / Head of Year (as in the section above) for investigation / action / sanction.
- Digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level *and only carried out using official school systems.*
- Online safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the school online safety policy.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Staff monitor ICT activity in lessons, extra curricular and extended school activities.
- Staff are aware of online 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.
- Remote access to the school server is done safely and without breaching the General Data Protection Regulation 2018 Confidentiality of staff and pupil information should be treated the same as if in the school building.

4.6 Designated Safeguarding Lead:

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

- social media
- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- sexting
- Radicalisation
- child sexual exploitation

4.7 Pupils:

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- Are educated on safe usage of social media / cyberbullying/ sexting/ grooming/ CSE/ radicalisation /digital social etiquette.
- 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 and the use of images.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

4.8 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' .

campaigns / literature. Parents and carers will be responsible for:

- Their child's use of digital technology outside of school.
- Endorsing (by signature) the Pupil Acceptable Use Policy.
- Accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

5.0 Policy Statements

5.1 Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in 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:

- A planned online safety programme should be provided as part of Computer Science/ PSHE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Annually using relevant outside agencies such as DSST.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- 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 helped to understand the need for the student / pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

5.2 Education – parents / carers:

Many parents and carers 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, VLE.
- Parents evenings.
- Parent sessions with DSST.
- Reference to suitable websites such as nspcc.org, thinkuknow.co.uk, saferinternet.org.uk

5.3 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. An audit of the online safety training needs of all staff will be carried out regularly. It is expected that some staff will identify online safety as a training need within the performance management process.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy.
- The Online Safety Champion will receive regular updates through attendance at SWGfL / LA / other information /training sessions and by reviewing guidance documents released by DSST/ SWGfL / LA and others.
- This Online safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Champion (or other nominated person) will provide advice / guidance / training as required to individuals as required.
- Follow up training will be provided to staff when the DSL/Online Safety Champion have been on relevant courses such as with DSST or CEOP.

5.4 Training – Governors:

Governors should take part in online safety training / awareness sessions, with particular importance for those who are responsible for overseeing 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.

6.0 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 Online safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Online Safety Champion and SLT.
- All users will be provided with a username and password by the school technician who will keep an up to date record of users and their usernames.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg 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
- 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 SLT.
- 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, the head teacher and ICT Co-ordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Champion and SLT.
- 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 online safety incident to the Network Manager (or other relevant person).
- 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, visitors) onto the school system.
- An agreed policy is in place 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.
- Personal data such as pupil records must not be kept on laptops and should only be accessed via the secure school server.
- An agreed policy is in place that allows staff to / forbids staff from installing programmes on school workstations / portable devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices.

- Memory sticks should not be used unless transferring files to a non-networked machine such as for assembly
- The school infrastructure and individual workstations are protected by up to date virus software.
- Instances of hacking or viruses, such as ransomware, must be reported immediately to the school technician, ICT Co-ordinator or SLT. This includes outside of school if the remote access is likely to have been compromised.

7.0 Curriculum:

Online safety should be a focus in all areas of the curriculum and staff 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, e.g. 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, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

8.1 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 media.
- 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. These images should only be taken on school equipment unless there is no alternative. In this instance direct permission must be been gained from the head teacher and all necessary precautions taken such as stringent checks by the network manager before and after use, no wifi enabled devises, all images to be removed and placed on the school network immediately after use, no images stored elsewhere.
- Only under extreme circumstances may images be taken on personal equipment without prior permission such as pupils safety being at risk. A member of the SLT must be informed directly after the event.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images (See Official Website Policy).
- Images can only be taken off site and used for educational purposes associated with the school

- Images should be kept on school owned computers and devices, unless there is no alternative available. In this instance permission must be sort from the SLT and the images must be removed as soon as possible.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers (See Official Website Policy).

8. 2 Use of Smart Technology

Smart technology implies the use of devices using mobile operating systems, such as tablets, phones and watches. These are becoming increasingly prevalent in the classroom. The use of phones, tablets and watches by pupils during school time is prohibited without permission of a teacher. The following rules apply to all members of staff or those working with children at Allenbourn

- Personal use of smart technologies is prohibited during lessons or in front of pupils.
- The use of smart technologies around pupils must be justifiable for educational purposes and included in planning where possible.
- Smart watches may be worn by members of staff, but must not have an inbuilt camera function.
- Pupils are not permitted to wear smart watches to school.
- No personal devices should be used by pupils, unless specific permission has been given by the head teacher.
- If permission has been given for pupils to use their own smart devices, it is the responsibility of the member of staff to remind pupils that the school holds no liability as issued in the home school agreement.
- If required, the school maintains the right to examine any smart technology used on the premises.
- If the personal use of smart technologies is considered or suspected of placing pupils' safety at risk, the police will be informed.
- If permission is given for a pupil to use their own smart device, including e-readers, these should not be internet enabled through 3G, 4G or equivalent.
- Members of staff who have a 3g/4g enabled device should only use these networks when there is no secure school wi-fi signal available.

8. 3 Pupil Mobile Phone Usage

- Pupils are permitted to bring phones to school but these must be switched off/silent and kept in their bags. No phones should be on open display and failure to do so will result in confiscation.
- The school holds no responsibility for any pupil's phone, which is broken, lost or stolen.
- Pupils are not permitted to use their phones during school hours unless a member of staff has granted permission. This should only be given if there are no other alternatives.
- Staff have the right to confiscate a pupil's phone in accordance to the searching, screening and confiscation at school guidelines under section 15 statuary guidelines for dealing with electronic devices.

9. 0 Data Protection

In accordance to the WAT GDPR policy, personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR) 2018 which requires data to be:

"(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

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.
- If leaving a computer for any duration it should be locked.
- Transfer data using encryption and secure password protected devices.
- When using remote access, staff must do everything reasonably possible to maintain confidentiality.
- No staff member should download or move any data from the school network using remote access.
- If a data breach occurs the SLT and Data Protection Officer must be informed immediately.
- In addition staff must fulfil all aspects of the WAT GDPR policy.

When personal data is stored on any portable computer system:
:

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

10.0 Communications

This is an area of rapidly developing technologies and uses.

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	Pupils

Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X						X	
Use of mobile phones in lessons				X				X
Use of mobile phones in social time	X							X
Taking photos on mobile phones				X				X
Smart watches may be bought to school	X							X
Use of smart watches in lessons				X				X
Use of smart watches in social time	X							X
Taking photos on a smart watch				X				X
Use of hand held devices eg e-readers, PDAs.	X						X	
Use of personal email addresses in school, or on school network		X					X	
Use of school email for personal emails				X				X
Use of chat rooms / facilities		X						X
Use of instant messaging				X				X
Use of social networking sites			X					X
Use of blogs		X				X		

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils 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 parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social

networking programmes must not be used for these communications (See Social Networking Policy).

- Individual educational email addresses and safe cloud services will be used with pupils.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- No member of staff should set up a personal email account related to the school or used for school business.

11.1 Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities eg Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those 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. If deemed unacceptable, staff disciplinary procedures will follow. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**child sexual abuse images**					X
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					X
	adult material that potentially breaches the Obscene Publications Act in the UK					X
	criminally racist material in UK					X
	pornography				X	
	promotion of any kind of discrimination				X	
	promotion of racial or religious hatred					X

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

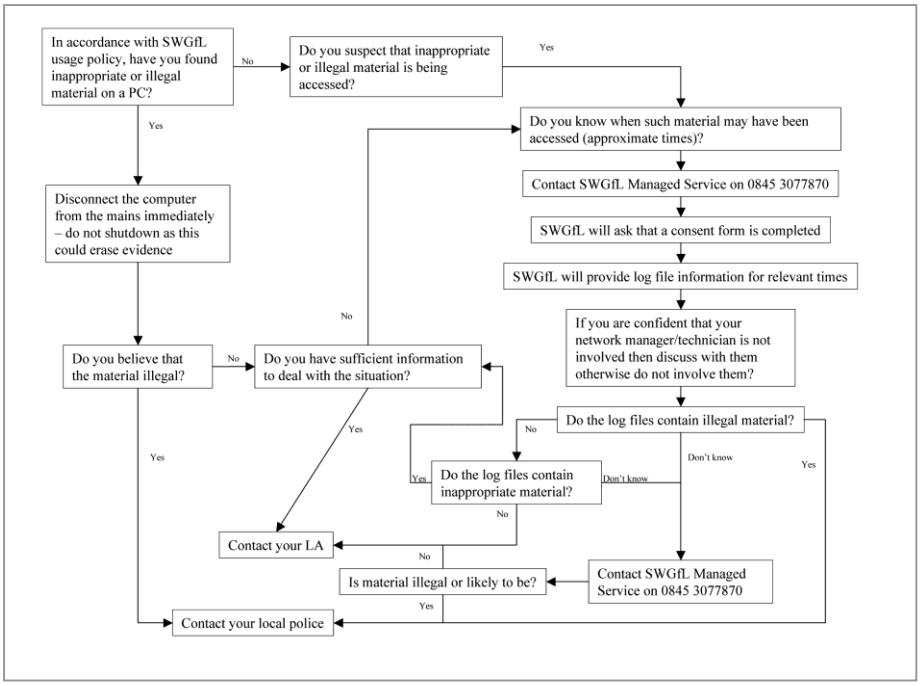
11.2 Responding to incidents of misuse

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 SWGfL flow chart – below and http://swgfl.org.uk/FAQs 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 Year / other	Refer to Head teacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X	X	X		X
Unauthorised use of non-educational sites during lessons	X	X						X	X
Unauthorised use of mobile phone / digital camera / other handheld device	X	X				X		X	
Unauthorised use of social networking / instant messaging / personal email	X							X	
Unauthorised downloading or uploading of files		X			X	X		X	X
Allowing others to access school network by sharing username and passwords	X	X			X		X	X	X
Attempting to access or accessing the school network, using another student's / pupil's account	X	X			X	X	X	X	X
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X		X	X	X	X	X
Corrupting or destroying the data of other users	X	X	X		X	X	X	X	X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X		X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system		X	X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X		X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X	X	X	X	X	X	X

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Head teacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action	Refer to DSL
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X			X	X	X
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		X	X		X	X	X	X	X
Unauthorised downloading or uploading of files	X	X	X	X	X	X	X	X	
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	X	X			X	X			X
Careless use of personal data eg holding or transferring data in an insecure manner	X					X			X
Deliberate actions to breach data protection or network security rules		X	X	X	X	X	X	X	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	X		X	X	X	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X	X	X		X	X	x	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X	X	X	X	X	X	X
Actions which could compromise the staff member's professional standing	X	X	X			X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X				X	X			
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X			
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X	X	X	X
Breaching copyright or licensing regulations		X	X	X	X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions		X	X	X	X	X	X	X	X

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online safety Policy Template:

- Members of the SWGfL Online safety Group and the SWGfL Online safety Conference Planning Group
- Avon and Somerset Police
- Somerset County Council
- Plymouth City Council
- Swindon Borough Council
- Poole Borough Council
- Bournemouth Borough Council
- North Somerset Council
- Gloucestershire County Council
- DCSF
- Becta
- National Education Network (NEN)
- London Grid for Learning
- Kent County Council
- Northern Grid for Learning
- Bracknell Forest Borough Council
- Byron Review – Children and New Technology – “Safer Children in a Digital World”