St Agnes ACE Academy E-Safety Policy

Content

Background / Rationale

The use of ICT 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
- The risk of being subject to grooming 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, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- 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.

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 understanding, confidence and skills to face and deal with these risks.

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by a working group made up of:

- School E-Safety Coordinator
- Headteacher
- Teachers
- Governors

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Governing Body on:	
The implementation of this e-safety policy will be monitored by the:	E-Safety Coordinator, Headteacher, Governing Body, E-Safety committee
The E-Safety Policy will be reviewed annually, 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:	6 month initial review and then annually
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LA ICT Manager LA Safeguarding Officer Police Commissioner's Office

The school will monitor the impact of the policy using:

- Logs of reported incidents
- SWGfL monitoring logs of internet activity (including sites visited)
- Surveys / questionnaires of
  - Pupils (e.g. Ofsted "Tell-us" survey / CEOP ThinkUknow survey)
  - Parents / carers
  - Staff

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the E-Safety Policy (on the recommendation of the E-safety Team) and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-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 Co-ordinator
- reporting to Governors

Headteacher

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator
- The Headteacher is 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

E-Safety Coordinator:

- leads the E-safety team.
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority when necessary and other agencies
- liaises with the school's ICT support providers to ensure that the school's ICT infrastructure is secure
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- keeps up to date with relevant E-Safety information in order to effectively carry out their e-safety role and to inform and update others as relevant
- Reports to the head teacher

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 and Head teacher for investigation / action / sanction
- Digital communications with students / pupils (email / Virtual Learning Environment ( ) should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in many aspects of the curriculum and other school activities
- Pupils understand and follow the school e-safety and acceptable use policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended school activities

Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, (embedded on computer sign in screen) which they will be expected to read before accessing the school systems.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents and carers will be responsible for:

- endorsing (by clicking OK on computer screen) the Student / Pupil Acceptable Use Policy
- Parents and cares will be encouraged to support the school/academy I promoting good e-safety practice and to follow guidelines on the appropriate use of:
    - Digital and video images taken at school events

Policy Statements

Education – Pupils

E-Safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of ICT / PHSE / other lessons and is regularly revisited (at the beginning of every half term and before each ICT lesson) this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages should be reinforced as part of a planned programme 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 helped to understand the need for the 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
- Rules for use of ICT systems / internet is displayed on log-on screens
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site,
- Parents evenings
- Reference to the appropriate websites

Education & Training – Staff

Staff training will be offered as follows:

- Regular E-Safety training will be made available to staff.
- New staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The E-Safety Coordinator will provide advice / guidance / training as required to individuals as required

Training – Governors

Governors will be invited to take part in e-safety training sessions, with particular importance for those who are members the E-Safety committee and child protection.

Technical – infrastructure / equipment, filtering and monitoring

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

- All users will be provided with a username and password by the e-safety coordinator.
- Access to the school ICT systems by "guests" (e.g. volunteer helpers) onto the school system is restricted. Visitors will be given a supply login to access a restricted version of our school system and they will not have access to areas which teachers have access to. Visitors will never use children's, staff or class log-ons

Trainee teachers will be given the same access to the schools systems as teachers with their own user name and password. They will read this policy and its appendix before using school ICT systems and sign the acceptable use agreement.

- The "master / administrator" passwords for the school ICT system, used by the ICT coordinator must also be available to the Head teacher.
- The school maintains and supports the managed filtering service provided by SWGfL and only the ICT coordinator, the Head teacher and the school's EduICT technician have the username and password to access the school's web filtering domain.
- 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 agreed to by the Head teacher.
- Any filtering issues should be reported immediately to SWGfL.
- Requests for sites to be removed from the filtered list will be considered by the ICT Coordinator and Head teacher, if the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Team.

Websites which are filtered may be accessed by staff using a staff proxy. Staff are prompted to enter a username and password when using a staff proxy. Staff will keep their username and password secure and notify the head teacher and ICT coordinator if they feel the security of their password and username has been compromised. Children and visitors will never be allowed to use the staff proxy

Staff are appropriately trained in the use of Staff Proxy used to bypass the school's filtering system. They are aware of the importance of closing web browsers after the school proxy has been used in order to prevent accidental access to unfiltered areas of the web. Staff are aware of the importance of checking websites that they may wish to access using the staff proxy first, before using them in the presence of children. The staff proxy may only be used for school/educational purposes and never for personal use.

- Staff will monitor the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Any actual, or potential, e-safety incident must be reported to the E-Safety Coordinator
- Staff use the network and ICT systems in line with the staff AUP
- The school infrastructure and individual workstations are protected by up to date virus software.

Communications

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

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x							x
Use of mobile phones in lessons				x				x
Taking photos of children on mobile phones				x				x
Use of hand held devices e.g. iPads, iPods	x				x			
Use of personal email addresses in school, or on school network	X Though not reccommended							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, eg, Twitter				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 are recommended to use the school email service to communicate with others when in school, or on school systems. Pupils will always do so in school and are encouraged to do so out of school.
- 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 students / pupils or parents / carers (email, chat, etc.) must be professional in tone and content. It is recommended that these communications should only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes should not be used for these communications.
- Whole class or group email addresses will be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses and encouraged to use these at home for the duration of their time at SAS. Once a child leaves SAS their email account will be deleted.

- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems.

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					x
	promotion or conduct of illegal acts, e.g. 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 (e.g. 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 e.g. You tube, Vimeo				x	

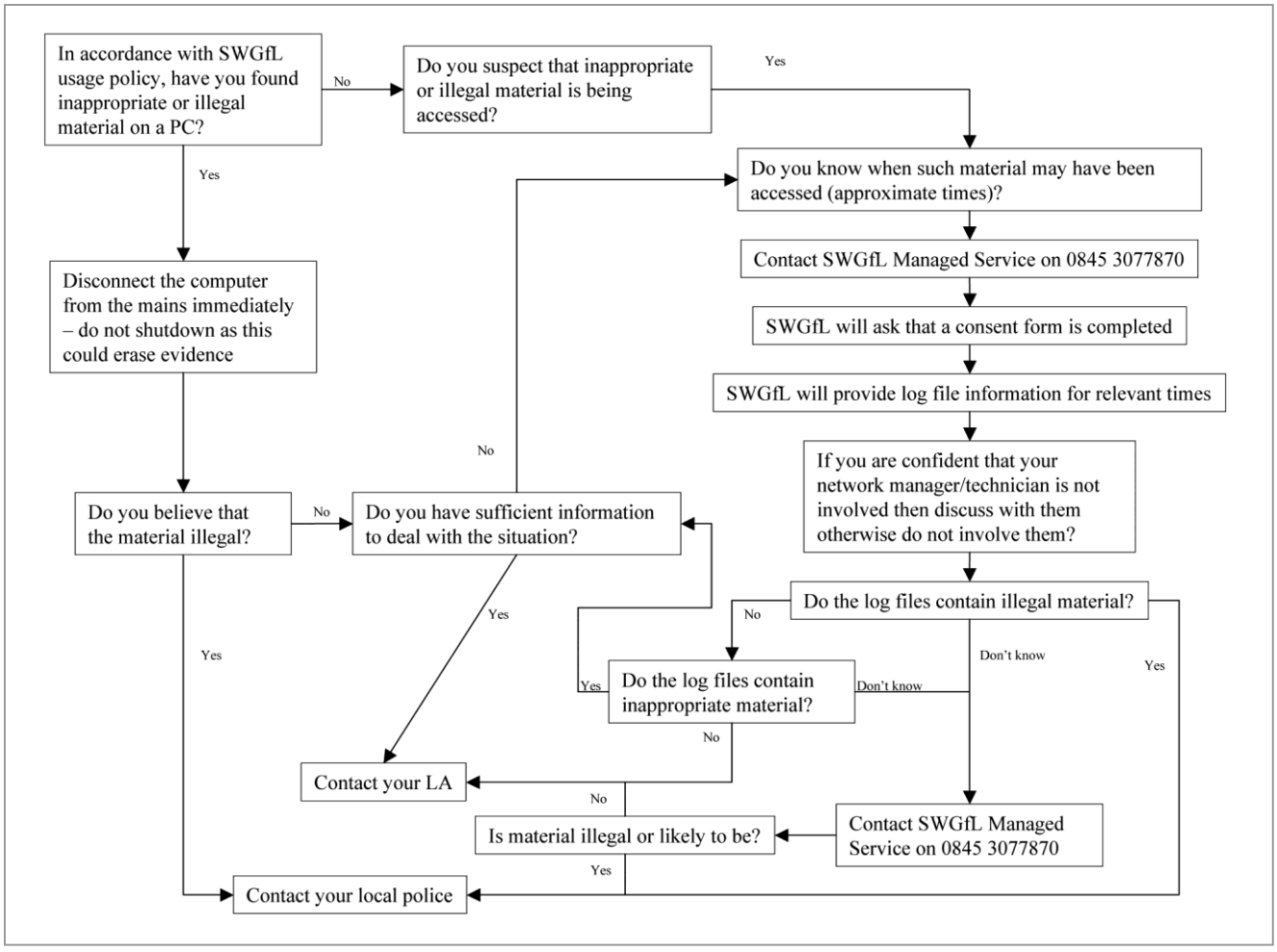
Responding to incidents of misuse

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

If any apparent or actual misuse appears to involve illegal activity i.e.

- 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://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.

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

Incidents:	Refer to class teacher / tutor	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security	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		
Unauthorised use of non-educational sites during lessons	x	x						
Unauthorised use of mobile phone / digital camera / other handheld device		x			x			
Unauthorised use of social networking / instant messaging / personal email		x			x			
Unauthorised downloading or uploading of files		x						
Allowing others to access school network by sharing username and passwords		x				x		
Attempting to access or accessing the school network, using another student's / pupil's account		x					x	
Attempting to access or accessing the school network, using the account of a member of staff		x				x		
Corrupting or destroying the data of other users		x				x		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		x			x		x	
Continued infringements of the above, following previous warnings or sanctions			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
Using proxy sites or other means to subvert the school's filtering system in order to provide educational material only		x			x	x		
Accidentally accessing offensive or pornographic material and failing to report the incident		x		x				
Deliberately accessing or trying to access offensive or pornographic material		x	x		x	x	x	x

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X			X		X	