e-safety Policy

Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within training environments and in their personal lives.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication learners 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 training providers are bound. The Academy's e-safety policy aims to ensure safe and appropriate use.

The use of these exciting and innovative tools in the Academy and at home has been shown to raise educational standards and promote learner achievement.

However, the use of these new technologies can put young people at risk within and outside the Academy or workplace. 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
- Radicalisation by extremist groups or individuals
- 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 e-safety policy is used in conjunction with other Academy 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 learners' 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.

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

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Senior Management Team and Board on	14th January 2016
The implementation of this e-safety policy will be monitored by the:	Safeguarding Co-ordinator reporting to the Senior Management Team
Monitoring will take place at regular intervals:	Annually
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	14th January 2017
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Safeguarding Officer, CEO Police Local Authority Designated Officer (LADO)

The Academy will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys of
  - Learners (QPD survey)
  - staff

Scope of the Policy

This policy applies to all members of the Academy including staff, learners, homestay providers, parents / carers, visitors, community users who have access to and are users of Academy ICT systems, both in and out of the Academy during learners' training blocks.

The Academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of Academy.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the Academy

The Board :

The Board will be updated with changes to the policy at regular meetings and will be required to approve any proposed changes or amendments to the policy by

- Regular meetings with the CEO

The Chief Executive Officer and Senior Management Team:

- The CEO is responsible for ensuring the safety (including e-safety) of members of the Academy community, though the day to day responsibility for e-safety will be delegated to the Safeguarding Co-ordinator.
- The CEO is responsible for ensuring that the Safeguarding 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 CEO / Senior Management Team will receive regular monitoring reports from Safeguarding Co-ordinator at monthly Head of Section meetings
- The CEO and Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see SWGfL flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures)

Safeguarding Coordinator with responsibility for E -Safety

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the Academy 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 Academy ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- meets regularly with CEO / SMT to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to CEO / SMT

IT Manager / Support Staff :

The IT Manager / Systems Manager is responsible for ensuring:

- that the Academy's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the Academy 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 Academy's networks through a properly enforced password protection policy, in which passwords are regularly changed
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Safeguarding Co-ordinator

Teaching and Support Staff

- they have an up to date awareness of e-safety matters and of the current Academy e-safety policy and practices
- they have read and understood and this e-safety policy document
- they report any suspected misuse or problem to the Safeguarding Co-ordinator / Chief Executive Officer
- digital communications with learners (email / Virtual Learning Environment (VLE) / voice**)** should be on a professional level and only carried out using official Academy systems
- e-safety issues are embedded in all aspects of the curriculum and other Academy activities
- learners understand and follow the Academy e-safety and acceptable use policy
- they monitor ICT activity in lessons, extra curricular and extended Academy 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 Academy policies with regard to these devices
- in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use

Learners

- are responsible for using the Academy ICT systems in accordance with the Learner Acceptable Use Policy, which they will be expected to sign before being given access to Academy systems
- 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 Academy policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand Academy policies on the taking / use of images and on cyber-bullying.

Communications

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

	Staff & other adults				Learners			
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 Academy	√					√		
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 Academy, or on Academy network						√		
Use of Academy email for personal emails	√							√
Use of chat rooms / facilities						√		
Use of instant messaging						√		
Use of social networking sites						√		
Use of blogs						√		

When using Academy technologies the Academy considers the following as good practice:

- **The official Academy email service may be regarded as safe and secure and is monitored**. Learners should therefore use only the Academy email service to communicate with others when in Academy, or on Academy systems (eg by remote access).
- **Users need to be aware that email communications may be monitored**

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					√
	accessing violent extremist websites, especially those with a social networking element;					√
	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 Academy or brings the Academy into disrepute				√	
Using Academy 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 Academy					√	
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 gambling					√	
On-line shopping / commerce					√	
File sharing					√	
Use of social networking sites					√	
Use of video broadcasting eg Youtube					√	

- Users must immediately report, to the Safeguarding Coordinator – in accordance with Academy 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 learners or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) Academy systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.

Unsuitable / inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and is banned from all Academy 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 the Academy context, either because of the age of the users or the nature of those activities.

The Academy believes that the activities referred to in the following section would be inappropriate in an Academy context and that users, as defined below, should not engage in these activities in the Academy or outside the Academy when using Academy equipment or systems. The Academy policy restricts certain internet usage as follows:

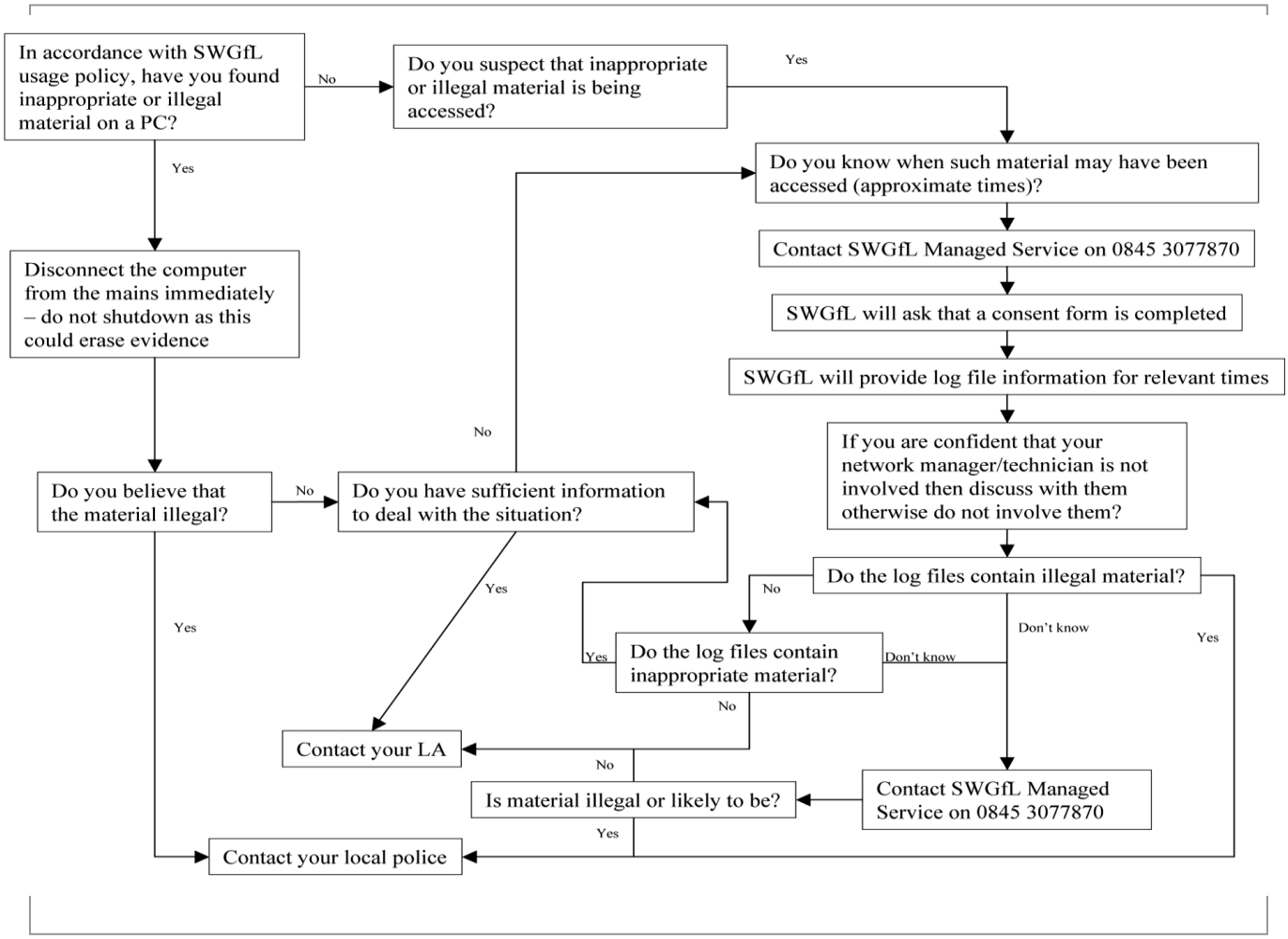
Responding to incidents of misuse

It is hoped that all members of the Academy 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://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.

Learners	Actions / Sanctions								
Incidents:	Refer to class Lecturer	Refer to Head of Curriculum	Refer to CEO	Refer to Safeguarding Coordinator	Refer to technical support staff for action re filtering / security etc	Inform employer	Removal of network / internet access rights	Warning	Further sanction eg 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 Academy network by sharing username and passwords	√								
Attempting to access or accessing the Academy network, using another learners account					√				
Attempting to access or accessing the Academy 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 Academy into disrepute or breach the integrity of the ethos of the Academy	√		√						
Using proxy sites or other means to subvert the Academy's filtering system	√					√			
Accidentally accessing offensive or pornographic material and failing to report the incident	√								

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Safeguarding Coordinator	Refer to CEO	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform employer	Removal of network / internet access rights	Warning	Further sanction eg 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	√				√				
accessing violent extremist websites, especially those with a social networking element;	√	√	√						
Attempting to access or accessing the Academy network, using learner's account	√				√				
Attempting to access or accessing the Academy 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 Academy into disrepute or breach the integrity of the ethos of the Academy			√						
Using proxy sites or other means to subvert the Academy;s filtering system			√		√				
Accidentally accessing offensive or pornographic material and failing to report the incident	√								

Date on which policy was approved: 14 01 2016

Policy review date: 14 01 2017

CEO ……..

Chair of Board……..