



E-SAFETY POLICY

Adopted on: 17th March 2016

Review Date: March 2017

Background / Rationale

E-Safety Definition

Safe use of electronic communication devices, including telephone, iPad, computer, internet and all mobile devices both in school and out of school. This policy serves to educate and protect staff, students and parents.

New technologies have become integral to the lives of children and young people in today's society, both within Pool Academy and in their lives outside the Academy.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students 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

The use of new technologies in our Academy and at home has been shown to raise educational standards and promote student achievement.

However, their use can put young people at risk within and outside the Academy.. 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
- Individuals or groups who use the Internet and digital technology to groom a young person into following their extremist ideas
- 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

Legal Policy

- 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 our e-safety policy aligns with other Academy policies (eg behaviour, anti-bullying and child protection policies).

As with all risks, it is impossible to eliminate those online completely. It is therefore essential, through good educational provision to build students' 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 Academy must demonstrate that it has provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. The e-safety policy that follows explains how we 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.

Development / Monitoring / Review of this Policy

The e-safety policy was developed by a group of staff and governors. Consultation took place with staff, student leadership group, governors, PTA and the wider community through the website and newsletters.

Schedule for Development / Monitoring / Review

The implementation of this e-safety policy will be monitored by the:	<i>Pool Academy E Safety Committee</i>
Monitoring will take place at regular intervals:	<i>Every Term</i>
The <i>Governing Body</i> will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	<i>Annually</i>
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:	<i>Annually</i>
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	<i>LA Safeguarding Officer –, Police Commissioner's Office, http://ceop.police.uk/CEOP</i>

The Academy will monitor the impact of the policy using:

- *Logs of reported incidents*

- *BT monitoring logs of internet activity (including sites visited)*
 - *Internal monitoring data for network activity*
 - *Surveys / questionnaires of*
 - *students (eg Ofsted “Tell-us” survey / CEOP ThinkUknow survey)*
 - *parents / carers*
 - *staff*
- The Red button App on iPads*
Timetabled random iPad checks every half term

Scope of the Policy

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

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 the Academy.

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. 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 / Officer*
- *regular monitoring of e-safety incident logs*
- *regular monitoring of filtering / change control logs*
- *reporting to relevant Governors committee / meeting*
- *The e-safety Governor is Frank Baker*

Principal and Senior Leaders:

- **The Principal is responsible for ensuring the safety (including e-safety) of members of the college community**, though the day to day responsibility for e-safety will be delegated to the *E-Safety Co-ordinator / Officer*.
- *The Principal / Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer 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 Principal / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in the Academy who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*
- *The Senior Leadership Team / Senior Management Team will receive regular monitoring reports termly from the E-Safety Co-ordinator / Officer via Lisette Neesham.*

- **The Principal and another member of the Senior Leadership 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 BT 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)
- The Business Manager is responsible for ensuring that the staff training record for Child Protection and e-safety is maintained up to date. A training audit is completed annually at the time of the completion of the S175 form.

E-Safety Coordinator / Officer:

- the e-safety officer is Lisette Neesham
- leads the e-safety committee
- 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 the Local Authority
- 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 E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The Network Manager is Phil Jones

The Network 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 BT 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
 - BT is informed of issues relating to the filtering applied by the Grid
 - the Academy's filtering policy is included in the appendix and updated on a regular basis and that its implementation is not the sole responsibility of any single person
 - that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- 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 E-Safety Co-ordinator / Head of ICT / ICT Co-ordinator / Class teacher / Head of House, Pastoral Support Managers for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in Academy policies

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current Academy e-safety policy and practices
- they have read, understood and signed the college Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator / Officer /Principal / Senior Leader / Head of ICT / ICT Co-ordinator / Class teacher / Head of House / Director of Learning (as in the section above) for investigation / action / sanction
- digital communications with students (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
- students understand and follow the Academy e-safety and acceptable use policy
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended college activities
- they are aware of e-safety issues related to the use of mobile phones, iPads, cameras and hand held devices and that they monitor their use and implement current college policies with regard to these devices
- in lessons where internet use is pre-planned students 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

Designated person for child protection / Child Protection Officer

The Designated Child Protection Officer is Lisette Neesham

The CP Trained staff are Lyndsey Trestrail, Sue Kent, Rod Peasley, Graham Carter, Nick Hamblin, Nigel Williams, Laura Peach, Nicki Carter, Zelma Hill, Claire Meakin and Lisette Neesham

The above staff should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

E-Safety Committee

Members of the E-safety committee (or other relevant group) will assist the E-Safety Coordinator / Officer (or other relevant person, as above) with:

- the production / review / monitoring of the Academy e-safety policy / documents.
- the production / review / monitoring of the Academy filtering policy (if the Academy chooses to have one)

Students

- are responsible for using the Academy's ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to Academy systems.
- 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 Academy policies on the use of mobile phones, iPads, digital cameras and hand held devices. They should also know and understand college policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of college and realise that the Academy's E-Safety Policy covers their actions out of the Academy, if related to their membership of the Academy.

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 Academy will therefore take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature*. Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy
- accessing the Academy website / VLE / on-line student / pupil records in accordance with the relevant Academy Acceptable Use Policy.

Community Users

Community Users who access the Academy ICT systems / website / VLE as part of the Extended Academy provision will be expected to sign a Community User AUP before being provided with access to Academy systems.

Policy Statements

Education – students

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

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

- A planned e-safety programme should be provided as part of ICT / PSHE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies inside and outside Academy
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students 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

- Students should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside the Academy
- Students 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 will be posted in all rooms
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

Many parents and carers have only a limited understanding of e-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.

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

- *Letters, newsletters, web site,*
- *Parents evenings*
- *Reference to the BT Safe website (nb the BT "Golden Rules" for parents)*

Education & Training – Staff

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

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the Academy e-safety policy and Acceptable Use Policies
- The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at BT / LA / other information / training sessions and by reviewing guidance documents released by NAACE / BT / LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training as required to individuals as required

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / e-safety / health and safety / child protection.

Technical – infrastructure / equipment, filtering and monitoring

The Academy will be responsible for ensuring that the Academy 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 e-safety responsibilities:

Legal Policy

- Academy ICT systems will be managed in ways that ensure that the Academy meets the e-safety technical requirements outlined in the BT Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of Academy ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted

- All users will have clearly defined access rights to Academy ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).
- All users will be provided with a username and password by The Network Manager who will keep an up to date record of users and their usernames.
- The “master / administrator” passwords for the Academy ICT system, used by the Network Manager (or other person) must also be available to the Principal or other nominated senior leader and kept in a secure place (eg Academy safe)
- Users will be made responsible for the security of their username and password. Users are responsible for their password being a “strong” password – please refer to the Network Manager for advice on password security. Users 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 Academy maintains and supports an internal filtering service. This filtering includes categories for pornographic material, extremist websites and other sites deemed not appropriate.
- 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 Principal (or other nominated senior leader).

- Staff have access to nearly unfiltered internet connections but this will still be monitored and reviewed. They are still filtered for illegal activity and extremism.
- Academy ICT technical staff regularly monitor and record the activity of users on the Academy ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Network Manager (or 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 Academy systems and data.
- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, visitors) onto the Academy system. That is they are given a temporary username and password.
- 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 / community users) and their family members are allowed on laptops and other portable devices that may be used out of the Academy. (see the Academy Personal Data Policy Template in the appendix for further detail)
- An agreed policy is in place that allows staff to install programs on Academy workstations / portable devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on Academy workstations / portable devices. (see Academy Personal Data Policy Template in the appendix for further detail)
- The Academy infrastructure and individual workstations are protected by up to date virus software.

- Personal data can not be sent over the internet or taken off the Academy site unless safely encrypted or otherwise secured. (see Academy Personal Data Policy Template in the appendix for further detail)

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- in lessons where internet use is pre-planned, it is best practice that students 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 students are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Students 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
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

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 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 Academy 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 students 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 eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow Academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Academy equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the Academy into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of students are published on the Academy website covered as part of the AUP signed by parents or carers at the start of the year see Parents / Carers AUP Agreement in the appendix.
- Student's / Pupil's work can only be published with the permission of the student and parents or carers.

PREVENT- Extremism and Intolerance

In line with the government's PREVENT strategy the school proactively monitors all digital communication for the promotion of terrorism or terrorist ideology and intolerance.

- All internet traffic on all devices in school and school devices at home is logged and recorded against the user.
- Sites promoting extremist views are blocked- this list is maintained by our filtering partner smoothwall and is updated constantly.
- Smoothwall provide safeguarding reports that are run weekly and detail any thing that might need further investigation. These are sent to the IT manager who then will raise it with the Safeguarding Lead if necessary.
- All email traffic is scanned for words and phrases relating to extremism, the grooming of children for extremist purposes and terrorism.
- The filter is flexible enough to allow the education of students the importance of safeguarding and the threats of these extremist groups in relevant lessons such as PSHE.

Data Protection

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

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

Staff must ensure that they:

- **At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**
- **Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.**
- **Transfer data using encryption and secure password protected devices**

Pool Academy does not permit students to use staff laptops or staff iPads under any circumstances.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with the Academy policy (below) once it has been transferred or its use is complete

Communications

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

Communication Technologies	Staff & other adults				Students			
	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 the Academy	x				x	x	x	
Use of mobile phones in lessons		x				x	x	
Use of mobile phones in social time	x				x			
Taking photos on school camera devices	x					x		
Taking photos on personal mobile phones				x				x
Use of hand held devices eg PDAs, PSPs	x					x	x	
Use of personal email addresses in the Academy, or on the Academy network		x						x
Use of the Academy email for personal emails that are within the teaching profession.		x				x		
Use of Academy email for personal emails not related to teaching .e.g. loans, dating sites etc				x				x
Use of non educational chat rooms / facilities				x				x
Use of educational chat rooms / facilities		x				x	x	
Use of instant messaging for education – Tutor Control/SIMS		x						x
Use of social networking sites using college equipment *				x				x
Use of educational blogs	x				x			
Use of non educational blogs				x				x

Legal Policy

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

- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the 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 students 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.
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the Academy website and only official email addresses should be used to identify members of staff.

*Guidance for Safer Working Practice for Adults who work with Children & Young People, DFES Publication, Jan 09, paragraph 13 . “ensure that if a social networking site is used, details are not shared with children and young people and privacy settings are set at a maximum”

Unsuitable / inappropriate 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:

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, 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	
Using Academy systems to run a private business					X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by BT and / or the Academy					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			

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 material**

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 Academy 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 Academy 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

Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of House / other	Refer to Principal / Deputy Headteacher	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
Unauthorised use of mobile phone / digital camera / other handheld device	X	X				X		X	X
Unauthorised use of social networking / instant messaging / personal email	X				X			X	X
Unauthorised downloading or uploading of files	X	X			X	X	X		X
Allowing others to access the Academy network by sharing username and passwords	X				X	X	X		
Attempting to access or accessing the Academy network, using another student's / pupil's account	X	X			X	X	X		X
Attempting to access or accessing the Academy network, using the account of a member of staff	X	X	X		X	X	X		X
Corrupting or destroying the data of other users	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
Continued infringements of the above, following previous warnings or sanctions	X	X	X		X	X	X		X
Actions which could bring the college into disrepute or breach the integrity of the ethos of the Academy	X	X	X		X	X	X		X
Using proxy sites or other means to subvert the Academy's filtering system	X	X			X	X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X	X	X	
Deliberately accessing or trying to access offensive or pornographic material	X	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

Staff

Incidents:	Refer to line management	Refer to Principal/Vice Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Disciplinary action
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
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	X	X	X			X
Unauthorised downloading or uploading of files	X	X	X		X	X
Allowing others to access the Academy network by sharing username and passwords or attempting to access or accessing the Academy network, using another person's account		X	X		X	X
Careless use of personal data eg holding or transferring data in an insecure manner	X		X		X	X
Deliberate actions to breach data protection or network security rules		X	X		X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		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
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students		X	X		X	X
Actions which could compromise the staff member's professional standing		X	X		X	X
Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the Academy	X	X	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
Breaching copyright or licensing regulations		X	X		X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X		X	X
Students as 'friends' on social networking sites		X				X
Parents as 'friends' on social networking sites		X				X

Any reference to school on ? social media ?

Appendices

Can be found on the following pages:

- (1) Student / Pupil Acceptable Usage Policy template 22
- (2) Staff and Volunteers Acceptable Usage Policy template 25
-
- (3) Academy Filtering Policy template 29
- (4) Academy Password Security Policy template 31
- (5) Academy E-Safety Charter 32

(1) Actioned each time a student logs onto the ICT system

(2) Needs to be completed annually and for any new staff

Student / Pupil Acceptable Use Policy Agreement

Academy Policy

New technologies have become integral to the lives of children and young people in today's society, both within the Academy and in their lives outside. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that Academy ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The Academy will try to ensure that *students* will have good access to ICT to enhance their learning and will, in return, expect the *students* to agree to be responsible users.

This agreement presented to all students every time they log into the school's ICT systems. They have to agree to it to get to the login screen and any further access.

Acceptable Use Policy Agreement

I understand that I must use Academy ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the college will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will not communicate with people I don't know in the "real world".
- I will not disclose or share personal information about myself or others when on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the Academy ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the college ICT systems for on-line gaming, on-line gambling or internet shopping will act as I expect others to act toward me:
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.

Legal Policy

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the Academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the Academy:

- I understand that, if I do use my own devices (such as USB sticks) in the Academy, I will follow the rules set out in this agreement, in the same way as if I was using Academy equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of the Academy:

- I understand that the Academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of the Academy and where they involve my membership of the Academy community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the Academy network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Staff (and Volunteer) Acceptable Use Policy Agreement Template

Academy Policy

New technologies have become integral to the lives of children and young people in today's society, both within academies and in their lives outside the Academy. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that Academy ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The Academy will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *students* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use the Academy ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the Academy will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of Academy ICT systems (eg laptops, email, VLE etc) out of the Academy
- I understand that the Academy ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the Academy.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I will adopt a "strong" password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using Academy ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the Academy's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the Academy website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

The Academy has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the Academy:

Legal Policy

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in the Academy, I will follow the rules set out in this agreement, in the same way as if I was using Academy equipment. I will also follow any additional rules set by the Academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant Academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not disable or cause any damage to Academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Academy / LA Personal Data Policy. Where personal data is transferred outside the secure Academy network, it must be encrypted.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Academy policy to disclose such information to an appropriate authority.

When using the internet in my professional capacity or for Academy sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the Academy:

- I understand that this Acceptable Use Policy applies not only to my work and use of college ICT equipment in the Academy, but also applies to my use of Academy ICT systems and equipment out of college and my use of personal equipment in the Academy or in situations related to my employment by the Academy.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the Academy ICT systems (both in and out of the Academy) and my own devices (in the Academy and when carrying out communications related to the Academy) within these guidelines.

Staff / Volunteer Name

Signed

Date

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students and members of staff may use digital cameras to record evidence of activities in lessons and out of the Academy. These images may then be used in presentations in subsequent lessons. Images may also be used to celebrate success through their publication in newsletters, on the Academy website and occasionally in the public media,

The Academy will comply with the Data Protection Act and request parents / carers permission before taking images of members of the Academy. We will also ensure that when images are published that the young people can not be identified by the use of their names. Parents are requested to sign the permission form on the back of the Admission Form at section J to allow the Academy to take and use images of their children.

The Academy Filtering Policy Template

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the Academy has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this Academy.

As a part of the BT academies and connected organisations automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

Responsibilities

The responsibility for the management of the Academy's filtering policy will be held by the Network manager. They will manage the college filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the BT / Academy filtering service must be only carried out by the ICT support staff.

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

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

Changes to the Filtering System

All staff have the right to ask the ICT support team for a site to be unfiltered or filtered, whether it be on a temporary or permanent basis. However, the final decision will rest with the Network Manager as to whether this will be implemented via the Pool Academy local filter.

Only sites with a relevant educational interest will be unfiltered.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The Academy will therefore monitor the activities of users on the Academy network and on Academy equipment as indicated in the Academy E-Safety Policy and the Acceptable Use agreement. Monitoring will take place as follows:

- All internet traffic is logged against the user and stored for 1 month.
- All emails are filtered for offensive words/language and attachments.
- Student user areas are monitored for offensive material.

Audit / Reporting

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

- E-Safety Committee
- Governors
- BT / Local Authority on request

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

The Academy Password Security Policy

Introduction

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

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

A safe and secure username / password system is essential if the above is to be established and will apply to all Academy ICT systems, including email and Virtual Learning Environment (VLE).

Responsibilities

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

All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. The only exception to this is the Curnow school student logins that are shared by a group of students.

Passwords for new users, and replacement passwords for existing users can be allocated by the ICT Support Team.

Users can change their passwords themselves at anytime via any Academy computer.

Training / Awareness

Members of staff will be made aware of the Academy's password policy:

- at induction

Legal Policy

- through the Academy's e-safety policy and password security policy
- through the Acceptable Use Agreement

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

- in ICT and e-safety assemblies
- through the Acceptable Use Agreement

Policy Statements

All users will have clearly defined access rights to the Academy ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).

All users will be provided with a username and password by the ICT support team.

The "master / administrator" passwords for the Academy ICT system, used by the Network Manager are also kept in the college safe in a sealed envelope. This must not be used unless there is no other way of contacting a member of the ICT support team.