Irlam & Cadishead College

2016 - 2017

E-Safety Policy

SALFORD ACADEMY TRUST

Review Date: October 2017

Policy Governance

This E-Safety Policy has been developed by:

E-Learning Coordinator	Mr N Ralph
E-Learning Coordinator Line Manager	Associate Senior Leader, Mr C Thomas
Designated Safeguarding Officer	Ms T Holdsworth

Schedule for Review

This E-Safety Policy was approved by the Governing Body on:	Transition Steering Group
The implementation of this E-Safety Policy will be monitored by:	Associate Senior Leader, Mr Thomas Assistant Principal & Designated Safeguarding Officer, Ms Holdsworth
Monitoring will take place at regular intervals:	Termly
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:	October 2017
Should serious e-safety incidents take place, the following persons should be informed:	Designated Safeguarding Officer People and Services Manager

Scope of the Policy

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

Roles and Responsibilities

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

Governors:

- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy

Principal and Senior Leaders:

- The Principal is responsible for ensuring the safety (including e-safety) of members of the College community
- 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

E-Safety Coordinator/Safeguarding Lead:

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the College 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

Network Manager/Technical staff:

The Network Manager is responsible for ensuring:

- That the College's ICT infrastructure is secure and is not open to misuse or malicious attack
- That the College meets the e-safety technical requirements outlined in the Salford City Council Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- That users may only access the College's networks through a properly enforced password protection policy

Teaching and Support Staff:

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current College 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 relevant person; in most cases this will be a student's teacher or Form Teacher; however for staff issues the Safeguarding Officer and the People and Services Manager should be informed. Investigation/action/sanction will then follow as appropriate.

Designated Safeguarding Officer:

They 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

Students:

- Are responsible for using the College ICT systems and mobile technologies in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to College systems – a record of this is kept in the Student Planner
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

Parents/Carers:

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

- Endorsing (by signature) the Student Acceptable Use Policy
- Accessing the College ICT systems or Learning Platform in accordance with the Student Acceptable Use Policy

E-Safety Education and Training

Education – Students:

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

- A planned e-safety programme will be provided as part of PHSE and will be regularly revisited – this will cover both the use of ICT and new technologies in and outside College
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students will 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

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 will receive e-safety training as part of their induction programme, ensuring that they fully understand the College E-Safety Policy and Acceptable Use Policies

Education and Training – Parents/Carers and Governors:

It is essential that Governors and parents/carers receive e-safety awareness and/or training and understand their responsibilities. Training will be offered as follows:

- A planned programme of e-safety awareness/ training will be made available to Governors and parents/carers

Communication Devices and Methods:

The following table shows the College's policy on the use of communication devices and methods.

Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the next table.

	Staff & Other Adults				Students			
Communication Method or Device	**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 College	x				x			
Use of mobile phones in lessons				x				x
Use of mobile phones in social time		x				x		
Taking photos or videos on personal mobile phones or other camera devices				x				x
Use of personal hand held devices (e.g. PSPs)		x						x
Use of personal email addresses in College, or on College network		x					x	
Use of College email for personal emails				x				x
Use of chat rooms/facilities		x						x
Use of instant messaging		x						x
Use of social networking sites		x						x
Use of blogs		x						x

This table indicates when some of the methods or devices above may be allowed:

	Circumstances when these may be allowed	
Communication Method or Device	**Staff & Other Adults**	**Students**
Mobile phones may be brought to College		To be switched off when students are in the College- only used outside during College break and lunchtime
Use of personal email addresses in College, or on College network	When essential to a Learning Objective	When essential to a Learning Objective
Use of chat rooms / facilities	When essential to a Learning Objective/For Safeguarding	
Use of instant messaging	When essential to a Learning Objective/For Safeguarding	
Use of blogs	When essential to a Learning Objective/For Safeguarding	

Unsuitable/Inappropriate Activities

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

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
User Actions					
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 based on race, gender, sexual orientation, religion and belief, age and disability					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 College or brings the College into disrepute				x	

Using College systems to run a private business				x	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SCC and/or the College				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	
Accessing the internet for personal or social use (e.g. online shopping, banking, etc.)				x	
File sharing (e.g. music, films, etc.)				x	
Use of social networking sites				x	
Use of video broadcasting (e.g. YouTube)				x	
Using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses)				x	

This table indicates when some of the methods or devices above may be allowed:

	Circumstances when these may be allowed	
User Actions	**Staff & Other Adults**	**Students**
Accessing the internet for personal or social use (e.g. online shopping, banking, etc.)	During recognised College break times	
File sharing (e.g. music, films etc.)	If copyright-free and essential to a Learning Objective	
Use of social networking sites	If essential to a learning objective, or to investigate incidents	
Use of video broadcasting (e.g. YouTube)	If essential to a learning objective	

Incident Management

Incidents (Staff and Community Users):	Refer to Curriculum Leader/ P&DL	Refer to Principal	Refer to Police	Refer to Technical Support Staff for action re filtering / security, etc.	Removal of Network / Internet Access Rights	Warning	Further Sanction
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		x	x				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	x						
Unauthorised downloading or uploading of files	x						
Allowing others to access College network by sharing username and passwords or attempting to access or accessing the College network, using another person's account		x					
Careless use of personal data (e.g. holding or transferring data in an insecure manner)	x						
Deliberate actions to breach data protection or network security rules	x						
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x						
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	x						

Using personal email / social networking / instant messaging / text messaging to carry out digital communications with students	x						
Actions which could compromise the staff member's professional standing	x						
Actions which could bring the College into disrepute or breach the integrity of the ethos of the College		x					
Using proxy sites or other means to subvert the College's filtering system	x						
Accidentally accessing offensive or pornographic material and failing to report the incident	x						
Deliberately accessing or trying to access offensive or pornographic material		x					
Breaching copyright or licensing regulations	x						
Continued infringements of the above, following previous warnings or sanctions		x					

Appendix 1 – Student Acceptable Use Policy

EMAIL & INTERNET ACCEPTABLE USE AGREEMENT

You must read and sign the Agreement before you can be allowed to use the internet or email at the College.

1. I understand that the College will monitor my use of the ICT systems, email and other digital communications.
2. I will only access those services I have been given permission to use. Games are not allowed unless they are educational and you have permission to take part.
3. I will not access the internet or emails for inappropriate purposes.
4. Any activities on the internet or email will be College work related.
5. I will not share my password with anyone else, nor will I interfere with anyone else's files, usernames or passwords.
6. I will not give any personal information including my name, address or telephone number to anyone via email.
7. I will not download, use or share any material which is subject to copyright. If in doubt, I will take steps to find out.
8. I will not view, upload or download or send by email any material which is likely to be unsuitable for children or colleagues. This applies to any material of a violent, dangerous, racist, homophobic or inappropriate sexual content. I will report any unpleasant or inappropriate material, messages or anything else that makes me feel uncomfortable.
9. I will be polite and responsible when I communicate with others. I will not use strong, aggressive or offensive language and I appreciate that others may have different opinions. Any comment made online will be treated the same as if you had said the comment out loud.
10. If you see any inappropriate use of school equipment or any inappropriate material online, it is your duty to report it.
11. The school keeps a log of all internet history. If you are found on inappropriate sites you will be issued with a sanction.

Sanctions

Failure to comply with these rules will result in one or more of the following:

1. A letter informing parents/carers of the nature of the ICT breach of rules.
2. Appropriate sanctions and restrictions placed on access to College facilities to be decided by a member of the Senior Leadership Team.
3. Any other action as decided by the Principal and/or the Governors of the College.

Signed:_____(Student) Date: _____

Print Name: _____ Year/Form: _____

Signed:_____(Parent) Date:_____

Appendix 2 – Use of Images Consent Form

CONSENT FORM

Consent form for Recording Images of Children

During your child's time with us we may wish to record images/film images and audio archives that involve your child. The images may be used for displays, publications and on websites by Irlam & Cadishead College or by local media/press.

Images and audio will only take place with the permission of the Operational Principal and under appropriate supervision. Students will only be named if there is a particular reason to do so (e.g. they have won a prize) and home addresses will never be disclosed. Images that may cause embarrassment or distress will not be used nor will images be associated with material or issues that are sensitive.

Before taking images and audio of your child, we need your permission. Please answer the questions below, then sign and date the form. You may ask to see images of your child at any time. Your permission may be withdrawn at any time.

I understand that:

The local media/press may take images and audio of activities to publicise the College and its students in a positive light e.g. drama performances or sporting events.

Photographers acting on behalf of Irlam & Cadishead College may take images for displays, publications or the College's website.

Embarrassing or distressing images will not be used.

The images will not be associated with distressing or sensitive issues.

The College will regularly review and delete unwanted materials.

I give my consent for images to be taken and used:	Please circle relevant answer	
a) Internally within the College	Yes	No
b) Including the child's name	Yes	No
c) Externally (e.g. within the media)	Yes	No
Name of person responsible for the child		
Signature of person responsible for the child		
Relationship to the child		
Date		

NB: There may be circumstances, beyond those above, in which images and audio of students are requested. The College recognises that in such circumstances specific consent from you will be required before recordings of students can be permitted.

Appendix 3 – Staff, Volunteer, Community User Acceptable Use Policy

College Policy

This Acceptable Use Policy (AUP) is intended to ensure:

- That staff, volunteers and community users will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use
- That College 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, volunteers and community users are protected from potential risk in their use of ICT in their everyday work

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

Acceptable Use Policy Agreement

I understand that I must use College 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 College 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 College ICT systems (e.g. laptops, email, VLE, etc.) out of College
- I understand that the College 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 College
- 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 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 College ICT systems
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions

- 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 College'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 (e.g. on the College website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use chat and social networking sites in College in accordance with the College's policies

- I will only communicate with students and parents/carers using official College systems. Any such communication will be professional in tone and manner.

- I will not engage in any on-line activity that may compromise my professional responsibilities

The College and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the College:

- When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices, etc.) in College, I will follow the rules set out in this agreement, in the same way as if I was using College equipment. I will also follow any additional rules in line with the College's E-Safety Policy set by the College 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 College 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 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 install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in College policies

- I will not disable or cause any damage to College 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 College/Local Authority Personal Data Policy. Where personal data is transferred outside the secure College network, it must be encrypted.

- I understand that data protection policy requires that any staff or student 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 College policy to disclose such information to an appropriate authority

- I will immediately report any damage or faults involving equipment or software, however this may have happened

When using the internet in my professional capacity or for College 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)

Staff, Volunteer and Community User Acceptable Use Agreement Form

This form relates to the Staff, Volunteer and Community User Acceptable Use Policy (AUP), to which it is attached.

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

- I understand that this Acceptable Use Policy applies not only to my work and use of College ICT equipment, but also applies to my use of College ICT systems and equipment out of College, as well as my use of personal equipment in College or in situations related to my employment by the College.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include 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 understood the College's E-safety Policy

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

Name	
Position	
Signed	
Date	