E-safety Policy

Irlam and Cadishead College

January 2017

SALFORD
ACADEMY TRUST

Policy Governance

Development, Monitoring and Review of this Policy

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

Position	Name(s)
E-Learning Coordinator	Mr N Ralph
E-Learning Coordinator Line Manager	Mr C Thomas

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

Forum	Date (if applicable)
Staff meetings	January 2017
School website	January 2017

Schedule for Review

This e-safety policy was approved by the Governing Body on:	
The implementation of this e-safety policy will be monitored by	Senior Leadership Team E-Learning Coordinator
Monitoring will take place at regular intervals:	Every 12 months
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:	December 2017
Should serious e-safety incidents take place, the following persons should be informed:	School Safeguarding Officer People and Services Manager

Scope of the Policy

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

Roles and Responsibilities

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

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 school community
- The Principal and another member of the Senior Leadership Team/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

E-Safety Coordinator/Officer:

This role is encompassed within the Safeguarding Officer SLT role.

- leads the e-safety committee and/or cross-school initiative on e-safety
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The Network Manager is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack

- that the school meets the 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 school's networks through a properly enforced password protection policy

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the relevant person; in most cases this will be a child's teacher or Form Teacher; however for staff issues the People and Services Manager should be informed. Investigation/action/ sanction will then follow as appropriate.

Designated person for child protection/Child Protection Officer

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/pupils:

- are responsible for using the school 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 school 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 school will take every opportunity to help parents understand these issues through parents' 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/Pupil Acceptable Use Policy
- accessing the school ICT systems or Learning Platform in accordance with the school Acceptable Use Policy.

Community Users

Community Users who access school ICT systems or Learning Platform as part of the Extended School provision will be expected to sign a Community User Acceptable Use Policy (AUP) before being provided with access to school systems.

E-Safety Education and Training

Education – students / pupils

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 school
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students/pupils 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 school e-safety policy and Acceptable Use Policies

Education and Training – Parents and Governors

It is essential that Governors and parents 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.

Communication devices and methods

The following table shows the school'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/Pupils			
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 school	☑				☑			
Use of mobile phones in lessons				☒				☒
Use of mobile phones in social time		⚠				⚠		
Taking photos or videos on personal mobile phones or other camera devices				☒				☒
Use of personal hand held devices eg PDAs, PSPs		⚠				⚠		
Use of personal email addresses in school, or on school network		⚠					⚠	
Use of school email for personal emails				☒				☒
Use of chat rooms / facilities		⚠					⚠	
Use of instant messaging		⚠					⚠	
Use of social networking sites		⚠						☒
Use of blogs		⚠					⚠	

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/Pupils**
Mobile phones may be brought to school		
Use of mobile phones in lessons		
Use of mobile phones in social time	During recognised College break times	During recognised College break times
Taking photos on personal mobile phones or other camera devices		
Use of personal hand held devices eg PDAs, PSPs	During recognised College break times or when essential to a Learning Objective	During recognised College break times
Use of personal email addresses in school, or on school network	When essential to a Learning Objective	When essential to a Learning Objective
Use of school email for personal emails		
Use of chat rooms / facilities	When essential to a Learning Objective	When essential to a Learning Objective
Use of instant messaging	When essential to a Learning Objective	When essential to a Learning Objective
Use of social networking sites		

Use of blogs	When essential to a Learning Objective	When essential to a Learning Objective

Unsuitable/inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school 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					☒
promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					☒
adult material that potentially breaches the Obscene Publications Act in the UK					☒
criminally racist material in UK					☒
Pornography					☒
promotion of any kind of discrimination based on race, gender, sexual orientation, religion and belief, age and disability					☒
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 school or brings the school into disrepute				☒	
Using school systems to run a private business				☒	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SCC and / or the school				☒	
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 gaming (educational)	☑				
On-line gaming (non educational)				☒	
On-line gambling				☒	

Accessing the internet for personal or social use (e.g. online shopping, banking etc)					
File sharing e.g. music, films etc					
Use of social networking sites					
Use of video broadcasting eg Youtube					
Using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses)	☑				

	Circumstances when these may be allowed	
User Actions	**Staff & other adults**	**Students/Pupils**
On-line gaming (educational)		
On-line gaming (non educational)		
On-line gambling		
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	If copyright-free and essential to a Learning Objective
Use of social networking sites	If essential to a learning objective, or to investigate incidents.	Not permitted on school network.
Use of video broadcasting eg Youtube	If essential to a learning objective,	YouTube not permitted. Other sites permitted if essential to a learning objective.
Using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses)		

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

Good practice guidelines

Email

Images, photos and videos

Internet

Mobile phones

SALFORD
ACADEMY TRUST

Social networking (e.g. Facebook/ Twitter)

Schools should take into consideration the age of their pupils, and whether they are old enough to have accounts when including this guidance.

Webcams

Incident Management

Incidents (students/ pupils):	Refer to class teacher	Refer to Curriculum Leader/ Progress & Development Leader	Refer to Principal	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
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		Yes							
Unauthorised use of non-educational sites during lessons	Yes								
Unauthorised use of mobile phone/digital camera / other handheld device		Yes							
Unauthorised use of social networking/ instant messaging/personal email		Yes							
Unauthorised downloading or uploading of files	Yes								
Allowing others to access school network by sharing username and passwords		Yes							
Attempting to access or accessing the school network, using another student's/pupil's account		Yes							
Attempting to access or accessing the school network, using the account of a member of staff			Yes						

Corrupting or destroying the data of other users		Yes							
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		Yes							
Continued infringements of the above, following previous warnings or sanctions			Yes						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			Yes						
Using proxy sites or other means to subvert the school's filtering system		Yes							
Accidentally accessing offensive or pornographic material and failing to report the incident		Yes							
Deliberately accessing or trying to access offensive or pornography		Yes							
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			Yes						

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)		Yes	Yes				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	Yes						
Unauthorised downloading or uploading of files	Yes						
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		Yes					
Careless use of personal data eg holding or transferring data in an insecure manner	Yes						
Deliberate actions to breach data protection or network security rules	Yes						
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		Yes					
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	Yes						
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	Yes						
Actions which could compromise the staff member's professional standing	Yes						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		Yes					

Using proxy sites or other means to subvert the school's filtering system	Yes						
Accidentally accessing offensive or pornographic material and failing to report the incident	Yes						
Deliberately accessing or trying to access offensive or pornographic material		Yes					
Breaching copyright or licensing regulations		Yes					
Continued infringements of the above, following previous warnings or sanctions		Yes					

Further information and support

For a glossary of terms used in this document:

http://www.salford.gov.uk/d/salford-esafety-glossary-jan2012.pdf

For e-Safety Practice Guidance for those who Work and Volunteer with, and have a Duty of Care to Safeguard Children and Young People:

http://www.salford.gov.uk/d/e-Safety-Practice-Guidance.pdf

R u cyber safe?

E-safety tips about how to stay safe online:

http://www.salford.gov.uk/rucybersafe.htm

Appendix 1 – Student/Pupil AUP

Student/pupil 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 – Staff, Volunteer, Community User AUP

Staff, Volunteer and Community User Acceptable Use Policy Agreement Template

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 communications 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 school 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/pupils 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 school 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 school ICT systems (eg laptops, email, VLE etc) out of school.
- 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 school'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 school 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 school in accordance with the school's policies.
- I will only communicate with students/pupils and parents/carers using official school 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 school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules in line with the School's E-Safety Policy set by the school 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 school 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 school policies
- I will not disable or cause any damage to school 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 School/Local Authority Personal Data Policy. Where personal data is transferred outside the secure school 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 school 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 school 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 student/pupil Acceptable Use Policy (AUP), to which it is attached.

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- 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 School's E-safety Policy**

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

Name	
Position	
Signed	
Date	

SALFORD ACADEMY TRUST

Appendix 3 – 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.