Name of Policy:E:Safety Policy
Date produced: Sept 2015
By: E Safety Coordinator
Last Review date: September 2018
Review date: September 2020

Development, Monitoring and Review of this Policy

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

Position	Name(s)
School E-Safety Coordinator / Officer	Richard Simcox
Headteacher	Jon Marsh
Head of ICT	Richard Simcox
Child Protection Officer	Melanie Howard
Governors	Mrs Nicola Anderson Co-Opted *(term from 13 Oct 2016 to 12 Oct 2020)* Miss Michelle Duval Co-Opted *(term from 13 Oct 2016 to 12 Oct 2020)* Mrs Anne Fallon Co-Opted *(term from 13 Oct 2016 to 12 Oct 2020)* Mr James Inman Headteacher *(term from 13 Oct 2016 to N/A)* Mrs Sharon Richardson Co-Opted *(term from 13 Oct 2016 to 12 Oct 2020)* Mr Ben Rockliffe Chair Co-Opted *(term from 13 Oct 2016 to 12 Oct 2020)* Mrs Anna Simmons Staff *(term from 13 Oct 2016 to 12 Oct 2020)* Mr Gareth Thompson Vice Chair Co-Opted *(term from 13 Oct 2016 to 12 Oct 2020)*
Parents and Carers	Mrs Mel Whittingham Parent *(term from 13 Oct 2016 to 12 Oct 2020*
Community Coordinator	Anna Simmons
ICT Advisor	RM

Schedule for Review

This e-safety policy was approved by the *Governing Body* on:	*Autumn 2015*
The implementation of this e-safety policy will be monitored by:	*ICT Strategy group*
Monitoring will take place at regular intervals:	*Half termly IT Strategy meetings*
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.	*Bi-annually*
Should serious e-safety incidents take place, the following Internal persons should be informed:	*DSL:- Melanie Howard* *James Inman (Executive headteacher)* *Jon Marsh (Head Teacher)*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*LA ICT Manager: David Rogers* *LA Safeguarding Officer: Patsy Malone* *Police*

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.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community
- The Headteacher 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:

The E-Safety Coordinator/Officer will work alongside Melanie Howard (the child protection officer) with day-to-day responsibility of e-safety.

- 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:

Managed Service provider (RM) and Salford City Council are 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 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 E-Safety Coordinator/Officer/Headteacher/Senior Leader/Head of ICT/ICT Coordinator/Class teacher/Head of House for investigation/action/sanction

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

E-Safety Committee

Members of the E-safety Committee will assist the E-Safety Coordinator/Officer *with* the production, review and monitoring of the school e-safety policy

Students/pupils:

- are responsible for using the school ICT systems and mobile technologies in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- 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 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 in accordance with the school Acceptable Use Policy.

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 ICT other lessons 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 online and be guided to validate the accuracy of information

E-Safety Rights Charter

1. You have the right to enjoy the internet and all the fun and safe things it has to offer.
2. You have the right to keep information about you private. You only have to tell people what you really want them to know.
3. You have the right to explore the internet but remember that you cannot trust everything that you see or read on the internet.
4. You have the right to know who you are talking to on the internet. You don't have to talk to someone if you don't want to.
5. Remember not everyone is who they say they are on the internet. You have the right to tell someone if you think anyone is suspicious. If you arrange to meet someone, tell a trusted adult or take a friend with you.
6. You have the right NOT to fill out forms or to answer questions you find on the internet.
7. You have the right NOT to be videoed or photographed by anyone using cameras, webcams or mobile phones.
8. You have the right NOT to have any videos or images of yourself put on the internet and you have the right to report it to an adult if anyone does this. (Remember that once images are posted online, they may not be able to be withdrawn).
9. You have the right NOT to be bullied by others on the internet and you have the right to report it to an adult if this happens.
10. If you accidentally see something you shouldn't, you have the right to tell someone and not feel guilty about it.
11. We are ALL responsible for treating everyone online with respect. You should not use behaviour or language that would be offensive or upsetting to somebody else.

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
- 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.

Staff

It is the responsibility of all adults within the school or other setting to:

- Ensure that they know who the designated person for Child Protection is within school or other setting so that any misuse or incidents can be reported which involve a child. Where an allegation is made against a member of staff it should be reported immediately to the Headteacher. In the event of an allegation made against the Headteacher, the Chair of Governors must be informed immediately.
- Be familiar with the Behaviour, Anti-bullying and other relevant policies so that in the event of misuse or an allegation, the correct procedures can be followed, immediately. In the event that a procedure is unknown, they will refer to the Headteacher immediately, who should then follow the Allegations Procedure, Section 12, LSCBN, where appropriate.
- Check the filtering levels are appropriate for their children and young people and are set at the correct level. Report any concerns to the E-safety Coordinators.
- Alert the e-Safety coordinator of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that students are protected and supported in their use of on-line technologies so that they know how to use them in a safe and responsible manner so that they can be in control and know what to do in the event of an incident.
- Be up-to-date with e-Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Sign an Acceptable Use Statement to show that they agree with and accept the rules for staff using non-personal equipment, within and beyond the school environment, as outlined in appendices.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998.Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in. The Business Manager will need to ensure that they follow the correct procedures for any data required to be taken from the school premises.
- Report accidental access to inappropriate materials to the e-Safety Coordinator and RM helpdesk in order that inappropriate sites are added to the restricted list or control this with the Local Control options via your broadband connection (through Community Gateway).

- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the Internet on a regular basis, especially when not connected to the school network.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies using the NCC accident/incident reporting procedure in the same way as for other non-physical assaults.

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.

Parents and School Community Support with E Safety

- Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

Managing E-safety Complaints

- Complaints of Internet misuse will be dealt with by a member of SLT.
- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Discussions will be held with the local Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.
- Sanctions within the school discipline policy include:
    - interview/counselling by the house co-ordinator;
    - informing parents or carers;
    - removal of Internet or computer access for a period.

Regulation and guidelines

The school's Internet access incorporates a software filtering system to block certain chat rooms, newsgroups, and inappropriate websites. The filtering system used on the school network aims to achieve the following:

- Access to inappropriate sites is blocked.
- Access will be allowed only to a listed range of approved sites.
- The content of web pages or web searches is dynamically filtered for unsuitable words.
- Records of banned Internet sites visited by students and teachers are logged.

Accessing a site denied by the filtering system will result in a report being generated and sent to the school's ICT Manager for appropriate action.

The school's ICT Manager regularly assesses the effectiveness of the filtering system. The school's filtering strategy is relevant to the pupils' age and requirements.

The school will immediately report the details of any inappropriate or illegal Internet material found to the Police or the child protection officer.

Similarly, the school will request of RM that 'allow' access be made of certain banned sites and provide the educational reasons behind the request.

E-mail accounts

Students may only use their approved e-mail account/s on the school network during school time.

Students shall immediately report any offensive e-mails that they receive to the teacher who will the report this to the ICT Manager and the ICT Coordinator.

Access in school to external, Web-based, personal e-mail accounts is denied for network security reasons.

It is forbidden to distribute chain letters or to forward a message without the prior permission of the sender.

Students must read their emails regularly and remove superfluous e-mails from the server.

Students may send spam messages only if they are required to do so as part of, for example, project work. Permission from the teacher will always be required to do this.

Students may not reveal their own or other people's personal details, such as addresses or telephone numbers or arrange to meet someone outside school via the school network.

Sending and receiving e-mail attachments is subject to permission from the teacher.

The school's website

An editorial team manages all aspects of placing web pages on the school's website. It has full editorial responsibility and ensures that the content on the site is accurate and appropriate. The website will comply with the Local Authority's guidelines.

The copyright of all material produced by the school for display on the school's web pages belongs to the school. Permission to reproduce any other material will be sought and obtained, from the copyright owner.

The contact details for the school will include only the school's postal address, e-mail address and telephone number. No information about teachers' home addresses or the like will be published.

The school will not publish any material produced by students without the agreed permission of their parents. In addition, photographs of students will not be published without a parent or carer's written permission.

Website photographs that include students will be carefully selected and will not be published without a parent or carer's written permission.

Moderated mailing lists, newsgroups and chat rooms

The school may use/uses an e-mail distribution list to send messages to selected groups of users.

Teachers will moderate other collaboration tools such as newsgroups and chat rooms if used on the school network for learning purposes.

Students will be denied access to public or unmoderated chat rooms.

Only regulated educational chat environments shall be used. They will always be used under supervision. Safety is the major consideration.

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 tablet devices		⚠					⚠	
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				☒				☒
Use of the school Twitter account.								☒

 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	School Phones used for photographing good practice.	
Use of mobile phones in social time	During breaks or after school	*During breaks or after school*
Taking photos on personal mobile phones or other camera devices		
Use of personal hand held devices.		
Use of personal email addresses in school, or on school network	During breaks or after school.	

Use of school email for personal emails		
Use of chat rooms / facilities		
Use of instant messaging		
Use of social networking sites		
Use of blogs		
Use of the school Twitter account.	Selected Staff using the Twitter Feed.	

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				☒	
Online gaming (educational)	☑				
Online gaming (non educational)					
Online 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**
Online gaming (educational)		
Online gaming (non educational)	After school clubs	After school clubs
Online gambling		
Accessing the internet for personal or social use (e.g. online shopping, banking etc)	During break times	
File sharing e.g. music, films etc	Only if copyright-free	Only if copyright-free
Use of social networking sites		
Use of video broadcasting eg Youtube	For showing educational videos	educational videos
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

Best practice

DO

Staff and students/pupils should only use their school email account to communicate with each other

Safe practice

Check the school e-safety policy regarding use of your school email or the internet for personal use e.g. shopping

Poor practice

DO NOT

Staff: don't use your personal email account to communicate with students/pupils and their families in accordance with the e-safety policy.

Buile Hill Academy

Images, photos and videos

Best practice

DO

Only use school equipment for taking pictures and videos.

Ensure parental permission is in place.

Safe practice

Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.

Delete images from the camera/device after downloading.

Poor practice

DO NOT

Don't download images from organisation equipment to your own equipment.

Don't use your own equipment in accordance with the e-safety policy.

Don't retain, copy or distribute images for your personal use.

Buile Hill Academy

Internet

Best practice

DO

Understand how to search safely online and how to report inappropriate content .

Safe practice

Staff and students/pupils should be aware that monitoring software will log online activity.

Be aware that keystroke monitoring software does just that. This means that if you are online shopping then your passwords, credit card numbers and security codes will all be visible to the monitoring technicians

Poor practice

DO NOT

Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings

Breach of the e-safety and acceptable use policies may result in confiscation of equipment, closing of accounts and instigation of sanctions.

Consilium Academies

Buile Hill Academy

Mobile phones

Best practice

DO

Staff: If you need to use a mobile phone while on school business (trips etc), the school will should provide equipment for you.

Make sure you know about inbuilt software/ facilities and switch off if appropriate.

Safe practice

Check the e-safety policy for any instances where using personal phones may be allowed.

Staff: Make sure you know how to employ safety measures like concealing your number by dialling 141 first

Poor practice

DO NOT

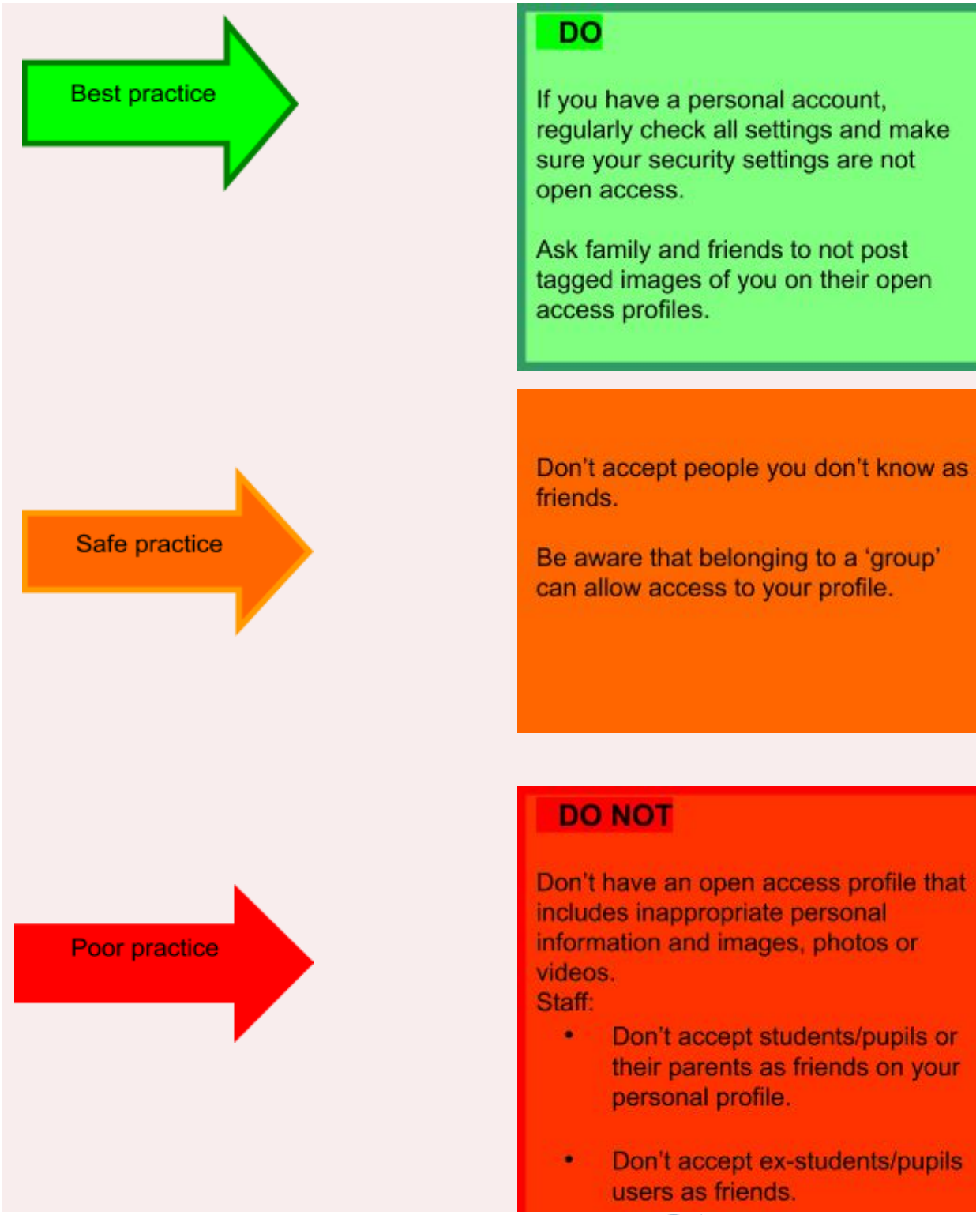
Staff: Don't use your own phone to contact parents or pupils.

Don't retain student/pupil/parental contact details for your personal use.

Consilium Academies

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.



Buile Hill Academy

Webcams

Best practice

DO

Make sure you know about inbuilt software/ facilities and switch off when not in use.

Safe practice

Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.

Delete images from the camera/device after downloading.

Poor practice

DO NOT

Don't download images from organisation equipment to your own equipment.

Don't use your own equipment in accordance with the e-safety policy.

Don't retain, copy or distribute images for your personal use.

Incident Management

Incidents **(students/pupils):**	Refer to class teacher	Refer to Head of Department / Head of Year / other	Refer to SLT/ Head	Refer to SLT /Head	Refer to technical support staff for action re filtering / security	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	/								
Unauthorised use of non-educational sites during lessons	/								
Unauthorised use of mobile phone/digital camera / other handheld device	/								
Unauthorised use of social networking/ instant messaging/personal email	/								
Unauthorised downloading or uploading of files	/								
Allowing others to access school network by sharing username and passwords	/								

Attempting to access or accessing the school network, using another student's/pupil's account	/								
Attempting to access or accessing the school network, using the account of a member of staff			/						
Corrupting or destroying the data of other users		/							
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature			/						
Continued infringements of the above, following previous warnings or sanctions			/						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			/						
Using proxy sites or other means to subvert the school's filtering system		/							
Accidentally accessing offensive or pornographic material and failing to report the incident			/						
Deliberately accessing or trying to access offensive or pornography			/						

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

Incidents (staff and community users):	Refer to Head of Department / Head of Year / other	Refer to Head	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)	/						
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	/						
Unauthorised downloading or uploading of files	/						
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	/						
Careless use of personal data eg holding or transferring data in an insecure manner	/						
Deliberate actions to breach data protection or network security rules	/						
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	/						
Sending an email, text or instant message that is regarded as	/						

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

Appendix 1 – Student/Pupil AUP

Student/pupil Acceptable Use Policy Agreement

Student/Pupil Acceptable Use Policy Agreement
This Acceptable Use Policy is intended to make sure:

- That you will be a responsible user and stay safe while using the internet and other technology for learning and personal use
- That ICT systems and users are protected from accidental or deliberate misuse

The school will try to ensure that you will have good access to ICT to enhance your learning and will, in return, expect you to agree to be a responsible user.

Please make sure you read and understand the following ☑ **I WILL** and ☒ **I WILL NOT** statements. If there's anything you're not sure of, ask your teacher.

Buile Hill Academy

I WILL:

- treat my username and password like my toothbrush – I will not share it, or try to use any other person's username and password
- immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online
- respect others' work and property and will not access, copy, remove or change anyone else's files, without their knowledge and permission
- 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
- only use my personal handheld/external devices (mobile phones/USB devices etc) in school if I have permission.
- understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment
- immediately report any damage or faults involving equipment or software, however this may have happened.

Consilium Academies

Buile Hill Academy

I WILL NOT:

- try (unless I have permission) to make downloads or uploads from the Internet
- take or share images (pictures and videos) of anyone without their permission
- use the school ICT systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.
- try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
- 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
- open any attachments to emails, unless I know and trust the person/organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes
- attempt to install programmes of any type on a machine, or store programmes on a computer
- try to alter computer settings

Consilium Academies

Student / Pupil 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, both in and out of school:

- I understand that the school 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 school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information)

- I understand that if I fail to follow this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Behaviour Consequences

Level	**Consequences**	**Strategies**	**Example behaviours**
Step 1	Official Warning	Classroom teacher based actions. strategies applied in the classroom by the classroom teacher – e.g. moved seating, redirecting to work, classroom support	Low level behaviours Talking not on task Repeated lateness
Step 2	Official Warning	Classroom teacher based actions Classroom teacher ensure sanctions are applied and completed Information entered onto SIMS if persistent as behaviour points	Repeated low level behaviours More serious behaviours preventing learning of the class
Step 3	Referred to HoD/HoF	Referral to Head of Department or faculty Students may be removed to work elsewhere within the department. Further sanctions applied.	Repeated disruption within the classroom despite management strategies.

		Parents informed by Teacher/HOY/HOF Classroom teacher enters information on SIMS Monitoring within subject area or faculty.	Complete refusal to comply. Serious incident.
Step 4	Referral to HoH/SID callout	Referral only done by Faculty leader Departmental sanctions applied and followed up – Departmental detention. Parents informed by HoY/HoF Parental meeting to discuss behaviour	Serious incident Continued or serious disruption of learning within the department despite management strategies.
Step 5	Referral to Seclusion	Referral to seclusion to Assistant headteacher – Ethos and RAC Behaviour Seclusion referral form completed and countersigned by HoY/HoF and parents interviewed. Seclusion – seclusion off site In extreme cases fixed term exclusion maybe considered	Serious incidents or repeated refusal to comply

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) eg mobile phones, PDAs, cameras etc
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, Learning Platform, website etc

(Parents/carers are requested to sign the permission form below to show your support of the school in this important aspect of the school's work).

Name of Student/Pupil		
Group/Class		
Signed (Student/Pupil)		Date
Signed (Parent/Carer)		Date

Appendix 2 – Staff & Volunteers.

Staff, Volunteer and Community User Acceptable Use Policy Agreement

School 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 school 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 / pupils

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 school 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 (e.g. laptops, email, RM Unify etc) out of school.
- I understand that the school 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 school.
- 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 school 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 / RM Unify) it will not be possible to identify by name, or other personal information, those who are featured.

- I will not 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 online 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 (Tablets/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 antivirus 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, Volunteers & 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	

Appendix 3 – Use of Images Consent Form

Use of Digital / Video Images

The use of digital/video images plays an important part in learning activities. Students/Pupils and members of staff may be using digital or video cameras to record evidence of activities in lessons and out of school. 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 school website and occasionally in the public media,
The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

Parents are requested to sign the permission form below to allow the school to take and use images of their children.

Permission Form

Parent / Carers Name	
Student / Pupil Name	

As the parent / carer of the above student / pupil, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of, school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed	
Date	