E-Safety and Acceptable Use Policy

Copley Junior School

Document Type	Policy
Document Ownership	Head teacher
Title of document	E-Safety and Acceptable Use Policy
Status	Final
Created by / Date	Head teacher, September 2018
Agreed by / Date	Curriculum and Standards sub committee, September 2018
Maintained By	Head teacher
Next Review Date	September 2020
Distribution	Network, Hard Copy in central file, Website
Master copy held	Network, Safeguarding folder
Replaces	E-Safety Policy 2017

E-SAFETY AND ACCEPTABLE USE POLICY

Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LA Safeguarding Unit on 01302 737777

Scope of the Policy

This policy applies to all members of the school community (including staff, 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 the 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.

Head teacher and Senior Leaders:

- The Head teacher is responsible for ensuring the safety (including e-safety) of members of the school community;
- The Head teacher and other members 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/Officer – Mrs E.A. Crayton:

- leads the e-safety 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 the Senior Leadership Team and Governors.

Network Manager / Technical Staff:

Doncaster LA, the school's chosen ICT support service, 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 Local Authority 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 E-Safety Co-ordinator/ Head teacher, Senior Leaders as appropriate for investigation/action/sanction.

Designated Leads for Child Protection – Mrs E.A. Crayton and Miss P. Havercroft:

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 online contact with adults/strangers;
- potential or actual incidents of grooming;
- cyber-bullying.

Pupils:

- are responsible for using the school ICT systems and mobile technologies in accordance with the 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/carers understand these issues through parents' evenings, newsletters, letters, the school website and information about national/local e-safety campaigns/literature. Parents and carers will be responsible for:

- endorsing the Pupil Acceptable Use Policy;
- accessing the school ICT systems in accordance with the school Acceptable Use Policy.

Community Users:

Community Users who access school ICT systems 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 – Pupils

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

- A planned e-safety programme will be provided as part of Computing/PSHCE/RSHE/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
- 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

Education and 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 periodically. It is expected that some staff may 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 and Acceptable Use Policy.

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.

Communication method or device	Staff and other adults				Pupils			
	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	☑							☒ Kept in office
Use of mobile phones in lessons				☒				☒
Use of mobile phones in social time	☑							☒
Taking photos on personal mobile phones or other camera devices				☒ See safe Practice p.10				☒
Use of personal hand held devices e.g. PlayStation Portable devices (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:

Communication method or device	Circumstances when these may be allowed	
	Teaching Staff and other adults	Pupils
Mobile phones may be brought to school	Must be put away during lesson times	Handed in to school office and locked away during the school day –only if mobile phone needed for going to a friend's after school, going to a parent's house etc.
Use of mobile phones in social time	e.g. during PPA breaks or after school	
Use of personal hand held devices e.g. e.g. PlayStation Portable devices (PSPs)	Allowed with Head's permission	
Use of personal email addresses in school, or on school network	e.g. during breaks or after school	
Use of blogs	Based on school projects	Based on school projects
Use of all above by the Senior Leadership team at the Head teacher's discretion		

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, e.g. 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 (e.g. 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					❌
On-line shopping / commerce for teaching resources			⚠️		
File sharing				❌	
Use of social networking sites				❌	
Use of video broadcasting e.g. YouTube			⚠️		
Accessing the internet for personal or social use (e.g. online shopping)			⚠️		
Using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses)		⚠️			

Good Practice Guidelines

Email

Best practice

☑ **DO**

Staff and 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 pupils and their families without a manager's knowledge or permission – and in accordance with the e-safety policy.

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 e.g. School Twitter.

Always make sure you have the Head teacher's/SLT's knowledge or permission.

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

Poor practice

☒ **DO NOT**

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

Don't use your own equipment without Head teacher/SLT knowledge or permission – and in accordance with the e-safety policy.

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

Internet

Best practice

☑ **DO**

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

Safe practice

⚠

Staff and pupils should be aware that monitoring software may log online activity.

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 policy may result in confiscation of equipment, closing of accounts and instigation of sanctions.

Mobile Phones

Best practice

☑ **DO**

Staff: With the Head teacher's permission you may use personal phones if you need to use a mobile phone while on school business (school visits etc.).
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 e.g. School Twitter.

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 without the Head teacher's/SLT's knowledge or permission.

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

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 Head teacher's/SLT's 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 the organisation's equipment to your own equipment.

Don't use your own equipment without the Head teacher's/SLT's knowledge or permission – and in accordance with the e-safety policy.

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

Incident Management

Incidents (Pupils):	Refer to class teacher	Refer to Head of Department / Head of Year / other	Refer to Head teacher	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 e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	X	X	X		X	X	2nd	1st	3rd
Unauthorised use of non-educational sites during lessons	X							X	
Unauthorised use of mobile phone/digital camera / other handheld device	X	X	X			X		X	
Unauthorised use of social networking/ instant messaging/personal email	No Access								
Unauthorised downloading or uploading of files	X				X			X	
Allowing others to access school network by sharing username and passwords	X				X			X	
Attempting to access or accessing the school network, using another pupil's account	X				X			X	
Attempting to access or accessing the school network, using the account of a member of staff	X		X		X			X	
Corrupting or destroying the data of other users	X		X		X			X	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	2nd	1st	3rd
Continued infringements of the above, following previous warnings or sanctions			X	X		X			
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X		X	X	2nd	1st	3rd
Using proxy sites or other means to subvert the school's filtering system			X		X		2nd	1st	3rd
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X			

Deliberately accessing or trying to access offensive material or pornography	X	X	X	X	X	X	2nd	1st	3rd
Receipt or transmission of material that infringes the copyright of another person or infringes the General Data Protection Regulations	X	X	X		X	X	2nd	1st	3rd

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

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

Pupil Acceptable Use of ICT Agreement

This Acceptable Use Policy is intended to make sure:

- That you will be a responsible user and stay safe whilst 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.

☑ 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. I 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

☒ 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 file sharing, or video broadcasting (e.g. 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 programs 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 programs
- attempt to install programs of any type on a machine, or store programs on a computer
- try to alter computer settings

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

- I understand that the school 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, exclusion, contact with parents/carers and, in the event of illegal activities, involvement of the police.

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) e.g. mobile phones, memory stick 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, website etc.

Name of Pupil		
Class		
Signed (Pupil)		Date

Staff, Volunteer and Community User Acceptable Use of ICT Agreement

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

- that staff, volunteers and community users will be responsible users and stay safe whilst 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 pupils learning and will, in return, expect staff, volunteers and community users to agree to be responsible users.

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 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, iPad, email, VLE 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 (e.g. on the school website / Twitter) it will not be possible to identify by name, or other personal information, those who are featured, unless permission has been given by a parent e.g. child receiving an award is featured in the local press and the parent wishes their child's name to be published alongside a photo.
- I will only communicate with 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 (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 use personal email addresses on the school ICT systems unless given permission by the Head teacher.
- 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 programs.
- 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 programs 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 programs of any type on a machine, or store programs 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 the General Data Protection Regulations (GDPR) require that any staff or 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).

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 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 and Acceptable Use 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	

Use of Digital / Video Images

Photographs of Children

Photographs and Videos of School Events

There are many occasions during the school year when we would like to take your child's photograph or to video school activities:

1. Photographs and videos taken by both staff and parents/carers at school events e.g. Harvest Festival, performances, special events, Sports Days, team photos at sports events etc.

2. Photographs of children's activities for displays and documents within the school e.g. assembly photos, workshops in school led by visitors, visits out of school, classroom activities etc.

3. Photographs of children alongside articles of school events in parish magazines, the 'Arrow' and the Free Press.

4. Photographs of children on the school website (please note that children's names will not be used alongside their photo). Photographs on the school website are changed and updated regularly; on some occasions, photos may remain on the website for a period of time for a specific purpose e.g. photos of the Year 6 annual residential visit, annual awards etc. remain on the website until the next year so they can be shared with the next cohort of pupils.

Please could **all parents/carers** fill in the attached reply slip if you are willing for your child's photograph to be taken. The permission you give will last for the time your child is in school, unless you inform us otherwise.

Parents/carers are welcome to take photographs at school events e.g. Harvest Festival, performances, Sports Days etc. and to video the events if you so wish. However, these photos must be for family enjoyment only and should not be copied or placed on the internet or **any** social networking sites such as Face book, Twitter, You Tube etc.

Please do not hesitate to contact us in school if there is anything else you would like to ask about these matters.

Photographs of Children

Photographs and Videos of School Events

I give/do not give (please circle as appropriate) my permission for my child to have his/her photograph taken whilst a pupil at Copley Junior School and for photographs of my child to be shared as detailed above. I understand that I understand that I may change my mind at any time but that it is my responsibility to notify the school in writing.

I wish to take photographs/videos of events organised by Copley Junior School.

I understand that in taking photographs/videos I am undertaking to abide by the restrictions of the school, namely that:

- The photographs/videos are for personal use only
- I will not allow anyone else to take copies of the photographs/videos other than close family members
- I will not put the photographs/videos on the internet or on **any** social networking sites such as Facebook, Twitter, You Tube etc.

Signed …………………………………………………………… (parent/carer)

Child's name ………………………………………………………………………….

Date………………………………………….

Policy reviewed and updated by all staff and governors of the Curriculum and Standards sub committee: September 2018