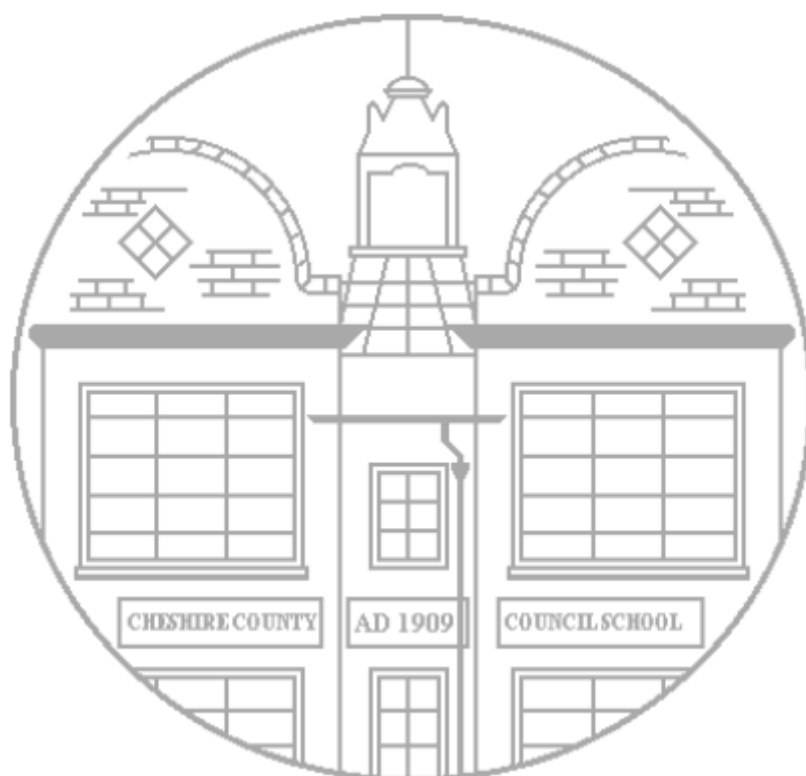# Cambridge Road Community Primary & Nursery School

E-Safety Policy

(Includes internet usage and acceptable Use Agreements)

Cambridge Road Community Primary & Nursery School

Cambridge Road Community Primary & Nursery School
E-Safety Policy

E-Safety and Internet Usage

E-safety includes internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's E safety policy will operate in conjunction with other policies including those for Behaviour, Anti-Bullying, Safeguarding, Child Protection, Data Protection and Image Consent form.

Why Is Internet Use Important?

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the internet is therefore an entitlement for pupils who show a responsible and mature approach to its use and Cambridge Road Community Primary and Nursery has a duty to provide pupils with internet access.

Many pupils will access the internet outside school and will need to learn how to evaluate online information and to take care of their own safety and security.

How Does Internet Use Benefit Education?

Benefits of using the internet in education include:

- access to world-wide educational resources including museums, libraries and art galleries
- rapid and cost effective worldwide communication
- inclusion in the National Education Network which connects all UK schools
- educational and cultural exchanges between pupils worldwide
- access to experts in many fields for pupils and staff
- professional development for staff through access to national developments, educational materials and effective curriculum practice
- collaboration across support services and professional associations
- improved access to technical support including remote management of networks and automatic system updates
- exchange of curriculum and administration data with the Local Authority
- access to learning wherever and whenever convenient
- greatly increased skills in Literacy

How Can The Internet Enhance Learning?

- The school internet access is designed for pupils' to use and includes filtering using SmoothWall for monitoring purposes.
- Children will be taught about acceptable internet use and given clear objectives for internet use.

Cambridge Road Community Primary & Nursery School
E-Safety Policy

- Internet use will be planned to enrich and enhance learning objectives
- Staff will guide pupils in online activities that are age appropriate and support learning activities

Good Practice

E-safety depends of effective practice at a number of levels:

- Responsible role models in school staff whom will use the internet correctly
- Implementation of E-safety policy in school
- Safe and secure internet access from the provider including the use of SmoothWall effectively

Dangers to be considered

Some of the dangers children may be face in relation to the internet may include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to or sharing of personal information
- The risk of grooming by others using the internet
- Sharing personal images without consent
- Inappropriate communication or interaction with others, including strangers
- Cyberbullying
- Access to inappropriate video or internet games
- An inability to be evaluate the quality, accuracy and relevance of information on the internet
- Risk of copyright infringement and plagiarism
- Illegal downloading or video or music
- Excessive use which can impact on social skills and personal development

It is impossible to alleviate all risk but as a school, it is essential that we teach children to have the skills to keep themselves safe. At Cambridge Road Community Primary School, we will provide the necessary safeguards to ensure we have done everything that can be reasonably done to help children identify, reduce and manage risk.

Cambridge Road Community Primary & Nursery School
E-Safety Policy

Below is a school self-audit to help SLT assess if E-safety basics are in place:

Does the school have an E-safety policy in place that complies with necessary government guidelines?	Yes
The policy is available to staff at:	http://www.cambridgeroad.cheshire.sch.uk/page/school-policies/36116
The policy Is available to parents at:	http://www.cambridgeroad.cheshire.sch.uk/page/school-policies/36116
The designated Child Protection contact is	Mr Darryl Pickering
The E-safety Coordinator is	Ms Louise Jones
The E-Safety Governor is	Mr Brad Lang (Chair)
E-safety training provided for both pupils and staff	Pupils through curriculum, PCSO and assemblies Staff through day to day support and through staff training days/twlights
Do children sign an agreement about responsible IT use? Are parents sent a copy of this?	Yes – included in permission booklet
Have school E-safety rules been set for pupils?	Yes
Are these rules displayed in all rooms with computers?	Displayed in ICT suite
Internet is provided by an approved educational internet service provider	Yes Local Government supply internet
Does the school regularly monitor internet usage using filters?	Yes – SmoothWall by E-safety officer
Is personal data collected, stored and used according to GDPR?	Yes

As a school, we will monitor the impact of this policy by:

- Logs of reported incidents
- E-safety coordinator and E-safety Governor will meet regularly to review monitoring
- Broadband monitoring through Local Government provider

Cambridge Road Community Primary & Nursery School
E-Safety Policy

Cambridge Road Community Primary and Nursery School has an appointed E-safety Coordinator Ms Louise Jones. The appointed E-safety Governor is Brad Lang (Chair).

Internet Access and Responsibility

- Parents are informed that pupils will be provided with supervised access to the internet.
- Parents will be sent a copy of the Pupil Acceptable Use Agreement vie permission and info booklet, which their children will have read with an adult and signed. (Appendix B)
- If staff or pupils find unsuitable sites, the site must be reported to the E-safety Coordinator who will investigate and if necessary get a block put in place for the site.
- Children will be taught skills to aid them in identifying the authenticity of material they may find on the internet.

Social Networking

- At our school, social networking sites are not available through pupil log in details and may only be accessed by adults using these for teaching or providing parents with school information.
- Children are advised never to give out their personal information of any kind, which may identify them or their location.
- Children are taught the importance of security and strong passwords along with how to act on unwanted content they may come across or receive.
- Children are taught the importance of only inviting people they know in real life versus on the internet to be part of their games or internet usage. They are also advised on how to report or block unwanted invites.
- Children and parents are advised on the relevance of age restrictions for social networking sites and the implications giving young children can have including dangers.

Filtering

Cambridge Road Primary uses the Local Government provider for internet access this includes using Smooth Wall to monitor and filter internet sites.

iPads and Mobile Phones

- Mobile phones will not be used for personal use during lessons and will be kept stored safely within allocated areas for adults belongings.
- iPads will be used to enhance teaching and within planned lessons towards the National Curriculum.
- iPads will be stored in allocated place within the school ICT room when not in use.
- Restrictions will be in place on the iPads to ensure only access to learning based content.

Cambridge Road Community Primary & Nursery School
E-Safety Policy

School Website

- Contact details on the web site is the school address, email and telephone number. No staff or children's personal information will be published.
- The head teacher will be responsible for content and editorial responsibility will be that of the Computing Coordinator or the admin team.

System Security

- School ICT capacity and security will be reviewed regularly.
- Virus protection will be installed across all ICT equipment and updated as necessary.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to GDPR and the Data Protection Act 1998.

Assessing Risk

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never be viewed on a school computer or device. The school cannot accept liability for the material accesse4d, or any consequences of internet access.
- The school will audit ICT use to ensure the E-safety policy is adhered to and adequate for its intention.

E-safety Complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints will be logged and dealt with as deemed appropriate by the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with the school child protection and safeguarding procedures.

Communication of E-safety Policy

- Pupils will sign and Acceptable Use Agreement.
- Rules for internet access will be available in areas were ICT equipment is accessed.
- Pupils will be informed their internet access and use will be monitored.
- Pupils will be reminded of E-safety rules regularly but especially when using the internet.

Staff

- All staff will be given a copy of the E-Safety Policy
- Staff should be aware that their internet use is monitored and traced to their individual log in credentials.
- Staff should use the lock screen facility when leaving their ICT equipment.

Cambridge Road Community Primary & Nursery School
E-Safety Policy

Appendices

Appendix A – Staff and Governor Acceptable Use Agreement

To ensure that all staff are fully aware of their professional responsibilities when using ICT, they are asked to read this code of conduct.

1. Aims and Backgrounds

This ICT user agreement covers the use of all digital technologies while in school: i.e. email, internet, network resources, learning platform, software, communication tools, social networking tools, school website, apps and any other relevant ICT systems provide by the school or Local Authority, or any other systems provided to be used by the school.

This ICT user agreement also covers post made on any non-school official social media platform or app, made from outside the school premises or school hours which reference the school or which might bring staff members or governors professional statue into disrepute.

2. User Requirements

School employees, governors and third party staff using school systems must comply with the requirements below. Failure to do so could possibly lead to disciplinary procedures.
Please note that school systems and users are protected and monitored by security and filtering systems to provide safe access to digital technologies. Your behaviour online when in school and on school devices whether in school or otherwise may be subject to monitoring.

a) I will only use the school's ICT resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body in the line of my employment.
b) I will set strong passwords, following advice provided by the school and technical support.
c) I will not reveal or share my password.
d) I will not uses anyone else's password(s) if they reveal them to me and will advise them to change it.
e) I will not allow unauthorised individuals to access email / internet / network / social networks / mobile apps / or any other system I have access to via the school or other authority or processing system.
f) I will ensure all documents, data, etc are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security policies (GDPR).
g) I will not engage in any online activity that may compromise my professional responsibilities.
h) I will only use approved methods of communicating with pupils or parents and will only communicate with them in a professional manner and on appropriate school business.
i) I will not support or promote extremist organisations, messages or individuals.
j) I will not give a voice or opportunity to extremist visitors with extremist views.
k) I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
l) I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Head.

m) I will not download any software or resources from the internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed. I will seek advice from the School Office.

n) I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.

o) I will not connect any device to the network that does not have up-to date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus and other malware systems.

p) I will follow the school's policy on use of mobile phones/devices at school.

q) I will only use school approved equipment for any storage, editing or transfer of digital images/videos and ensure I only save photographs and videos of children and staff on the appropriate system or staff-only drive within school.

r) I will only I take or publish images of staff and students with their permission and in accordance the school's consent guidelines. Images published on the school website, online learning environment etc. will not identify students by name, or other personal information.

s) I will use the school's Learning Platform or online cloud storage service in accordance with school protocols.

t) I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role, and will create a distinction between the two.

u) I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.

v) I agree and accept that any computer or laptop or memory stick loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.

w) I will only access school resources remotely (such as from home) using the school approved system and follow e-security protocols to interact with them.

a) I will ensure any confidential data that I wish to transport from one location to another is protected and that I follow school data security protocols when using any such data at any location.

b) I understand that data protection policy (GDPR) requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

c) I am aware that under the provisions of the GDPR (General Data Protection Regulation), my school and I have extended responsibilities regarding the creation, use, storage and deletion of data, and I will not store any pupil data that is not in line with the school's data policy and adequately protected. The school's data protection officer must be aware of all data storage.

d) I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the relevant Senior Member of Staff / Designated Safeguarding Lead. I understand that all internet and network traffic / usage can be logged and this information can be made available to the Head / Safeguarding Lead on their request.

e) I understand that internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.

f) I understand that I have a responsibility to uphold the standing of the teaching profession and of the school, and that my digital behaviour can influence this.

g) I will embed the school's online safety / digital literacy / counter extremism curriculum into my teaching.

Links with Other Policies

I understand that this user agreement is linked to the schools:

- Online and E-Safety Policy

- GDPR/Data Protection Policy

- Safeguarding and Child Protection Policy

Appendix B

Acceptable Use Agreement for KS1

- I will use the school computers and technology sensibly.
- I will only use the internet or computer when a teacher or adult is with me.
- I will only use my own login and password and I will not tell anyone else what it is.
- I will not look at or delete other people's files.
- I will not bring in memory sticks from home without permission.
- If I see anything that upsets me, I will tell an adult.
- I will not give out any details about me – like my name or address.
- I know school will check my computer and be able to see what I am doing and what sites I have visited.
- If I break these rules I know I may be stopped from using the internet and/or computers.

Acceptable Use Agreement for KS2

- I will use the school computers and technology sensibly.
- I will ask permission from an adult before I look at the internet.
- I will only log on using my own username and password which I will keep confidential.
- I will only look at my own work and not delete anyone else's files.
- I will not bring in a USBs from home without permission.
- I will only email people I know.
- I will always be polite and use appropriate language when emailing or sending messages on the computer.
- I will not give out my personal information or arrange to meet anyone.
- If I think anything on the internet upsets me or a stranger sends me a message, I will tell an adult.
- I know school will check my computer and be able to see what I am doing and what sites I have visited.
- If I break these rules I know I may be stopped from using the internet and/or computers

Cambridge Road Community Primary & Nursery School
E-Safety Policy

Dear Parents

In school we have access to the internet. This is a powerful tool which opens up new opportunities for everyone and promotes effective learning. At Cambridge Road we are aware that young people should have an entitlement to safe internet access at all times. However, school and parents have a duty of care to protect children and ensure that internet use is responsible and safe.

We strongly recommend that children do not use social network sites such as Facebook, Instagram, Snapchat, Tiktok or have YouTube accounts at home. These carry an age-restriction of 13 years old and pose a risk to children. Social networks have no place in our school and so school staff should not be approached by pupils or parents online or invited to join.

Your child has read the following **Acceptable Use Agreement** in class with their teacher. Once they have fully understood them all, your child has signed their name to agree to stick by them. Please read them again at home with your child to show your support of the school in this important aspect of our work. Thank you.

- I will use the school computers and technology sensibly
- I will ask permission from an adult before I look at the internet
- I will only log on using my own username and password which I will keep confidential
- I will only look at my own work and not delete anyone else's files
- I will not bring in a USBs from home without permission
- I will only email people I know
- I will always be polite and use appropriate language when emailing or sending messages on the computer
- I will not give out my personal information or arrange to meet anyone
- If I think anything on the internet upsets me or a stranger sends me a message, I will tell an adult
- I know school will check my computer and be able to see what I am doing and what sites I have visited
- If I break these rules I know I may be stopped from using the internet and/or computers

Appendix D

Use of Communication and Information Technology in School

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

Communication Technologies	Staff & other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Mobile phones may be brought to school	*							*
Use of mobile phones in lessons				*				*
Use of mobile phones in social time	*							*
Taking photos on mobile phones				*				*
Use of school hand held devices e.g. iPads	*						*	
Use of personal email addresses in school, or on school network	*							*
Use of chat rooms/facilities				*				*
Use of instant messaging				*		*		
Use of social networking sites				*				*
Use of blogs				*		*		
Use of secure learning platforms to collaborate	*				*			

When using email the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored
- Users must immediately report, to the nominated person – in accordance with the school policies, the receipt of any email or electronic message that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and parents must be professional in tone and content

- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.