Cavendish Community Primary School

Acceptable Use Policy - Adults

We believe that the use of technology plays a crucial role in the delivery, planning, assessment and enrichment of children's learning and our school's interactions with the outside world. Therefore, it is imperative that the adults who work with the children at Cavendish Community Primary School engage with all forms of technology in a confident, creative and appropriate manner.

This policy aims to set out the actions the school takes to ensure that all adults at school can meet these expectations and the responsibility adults at school have to use technology in an appropriate manner, as set out in this policy.

The school will:

- Provide suitable devices for staff to use in planning, delivering, assessing and reporting on children's learning. These devices remain the property of the school and can be recalled and checked at any time. These devices must be password/fingerprint protected.
- Provide and maintain the school network so that it supports the core business of the school. The network systems and internet systems are filtered via One Education using *Sophos XGS Firewall*..
- Exercise its right to monitor the use of information systems and internet systems, and to intercept and delete inappropriate materials where it believes unauthorised use of the systems may be taking place, or to maintain as evidence where the system may be being used for criminal purposes or for storing unacceptable, unauthorised or unlawful text or imagery within the context of 'Keeping Children Safe in Education – Annex C' DfE September 2023. An organisation called Smoothwall monitors our network on our behalf.
- Provide all adults and children (when at an appropriate age) with a unique log in to access the network with.
- Ensure there is suitable and developmental training for adults and a named member of staff to monitor curriculum provision.

Adults at school will:

- Use the technology available at school to enhance teaching and learning and to help safeguard children's safety.
- Be open to new technology and any training associated with it.
- Use any devices given to them by school (laptops, iPads, mobile phones) in an appropriate and professional manner and with due regard to GDPR regulations. These devices can be connected to home wifi networks. These devices should be returned to school whenever requested and in the event of an employee leaving the school.
- Use their own devices in school in an appropriate and professional manner and with due regard to GDPR regulations. Colleagues are allowed to have their own mobile devices in school and to connect them to the school wifi network. The use of personal mobile phones whilst working with children is strictly prohibited. If personal phones have to be used for any purpose, they should be used in staff areas or empty classrooms during set breaktimes only. **Failure to adhere to this guidance could lead to disciplinary action being taken.**
- Only use school devices to make digital images of the children. These images should be saved to the school network and deleted from the device as soon as possible.
- Report any use of technology which goes against the guidance contained in this document, either by adults or children.
- Ensure that children are not given unsupervised access to the Internet. For the purposes of this policy, "supervised" means that the user is within direct sight of a responsible adult.
- Teach Internet safety in keeping with the school's Computing Scheme of Work, but all teachers within all year groups should be including Internet safety as part of their discussions on the responsible use of the school's computer systems. In addition, each phase of school will have a half termly e-safety assembly.
- The use of re-writeable CDs, memory sticks etc. to transfer data from external computer systems is **forbidden**. Where information has been downloaded from the internet, or copied from another computer, wherever possible it must be emailed to school to ensure that it undergoes anti-virus scanning. If this proves to be impossible, (due to file size, technical difficulty etc.) express permission must be sought from the ICT co-ordinator prior to the data being transferred.
- To be read in conjunction with *Social Media Policy*.

Responding to inappropriate use of the Cavendish ICT Systems

Any incidents of inappropriate use will be reported to the head teacher and documented along with any actions taken. The school may remove ICT access, temporarily or permanently, from anyone it believes to have purposefully broken the rules set out in this document, and the individual concerned may be subject to disciplinary procedures.

The school also has a duty to pass on any information about the possession of inappropriate content to the police - in the case of inappropriate use from a child, the parents/carers of the child will be informed.

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on any school computer. Neither Cavendish Community Primary School nor Manchester City Council can accept liability for the material accessed, or any consequences of Internet access.

APPENDIX

E-safety Curriculum Overview - EVOLVE

Year Group	Autumn 1	Autumn 2	Spring 1	Internet Safety Week (Feb)	Spring 2	Summer 1	Summer 2	Wellbeing Week (July)
	Strand of Learning – Project Evolve Toolkit							
	Self-Image & Identity	Online Bullying	Copyright & Ownership	Privacy & Security	Managing Online Information	Online Relationships	Online Reputation	Health, Wellbeing and Lifestyle

https://projectevolve.co.uk/toolkit/resources/

What is ProjectEVOLVE?

ProjectEVOLVE resources each of the 330 statements from UK Council for Internet Safety's (UKCIS) framework "Education for a Connected World" with perspectives; research; activities; outcomes; supporting resources and professional development materials.

This vast library of content is managed by an innovative new engine, designed by the brilliant SWGfL Webteam, that not only makes navigating the content intuitive but allows users to personalise the content they collate.

The vibrant new content has been written by a team of experts here at the UK Safer Internet Centre. It's up to date; relevant and engaging and moves online life education into the third decade of the 21st century.

Links to SDP – priority 3: brilliantly happy, healthy & safe

KCSIE reference

Online safety

135. It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

136. The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

contact: being subjected to harmful online interaction with other users; for example:

peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

commerce: risks such as online gambling, inappropriate advertising, phishing and or 38Public Health England: has now been replaced by the UK Health Security Agency and the Office for Health Improvement and Disparities (OHID), which is part of the Department of Health and Social Care, and by the UK Health Security Agency, however branding remains unchanged. 36 financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Primary School Focus (as in line with the areas of risk from KCSIE) -

CONDUCT	How children behave online and interact themselves. This is about keeping their information secure, being responsible for their own health and well-being (not spending excessive time online or gaming), considering their digital footprint and online reputation.
CONTENT	Children being exposed to harmful, illegal or inappropriate material. Examples such inappropriate material, ignoring age ratings on games, films and television programmes.
CONTACT	Children being subjected to harmful online interaction with others. Examples include grooming (an adult pretending to be a child), any form of online bullying through social media sites, identify theft.