Cannon Park Primary School

Encouraging Excellence

Online Safety Policy

Review Programme:	
Policy Adopted	March 2014
Policy Review Date	December 2024
Date of Next Review	October 2025
Reviewed by	Mr. James Young
Head Teacher	Mr. Tom Ray
Chair of Governors	Mr. J. Teago

This policy has been reviewed; to the best of our knowledge we do not feel it impacts negatively on any specific group or individual within our school community

The aim of online safety at Cannon Park

Use of the internet is an integral part of our learning philosophy at Cannon Park Primary School. Whilst the internet offers many educational benefits across the curriculum, its use necessitates a clear policy due to the nature in which the digital space continues to grow. To keep children safe, this document sets out clear guidelines to help ensure that our whole school approach is consistent and functions in tandem with our Child Protection Policy. The 4Cs listed below also highlight the key areas that staff are aware of and have regular training on in order to identify signs of abuse.

The 4Cs:

The breadth of issues classified within the 4Cs is considerable and ever evolving, but can be broadly categorised as follows:
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 non-consensual 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 financial scams.

Safeguarding, Online and offline:

All staff are aware that technology can be a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online (child-on-child abuse), this can take the form of

• bullying (including cyberbullying, prejudice-based and discriminatory bullying)

• abuse in intimate personal relationships between children (sometimes known as 'teenage relationship abuse')

• physical abuse such as hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm (this may include an online element which facilitates, threatens and/or encourages physical abuse)

• sexual violence such as rape, assault by penetration and sexual assault; (this may include an online element which facilitates, threatens and/or encourages sexual violence)

- sexual harassment such as sexual comments, remarks, jokes and online sexual harassment, which may be standalone or part of a broader pattern of abuse

• causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party

• consensual and non-consensual sharing of nude and semi-nude images and/or videos11 (also known as sexting or youth produced sexual imagery)

• up skirting which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress, or alarm, and

• initiation/hazing type violence and rituals (this could include activities involving harassment, abuse or humiliation used as a way of initiating a person into a group and may also include an online element).

Staff attend regular CPD sessions to remain up to date in technological advances and changes to the Keeping Children Safe in Education document so that they can enact best practice to prevent and/or identify abuse linked to online issues.

Acceptable use:

Pupils will only interact with electronic devices authorised for use at school including tablets and chrome books. The children do not use or bring in their own mobile phones or smart watches under any circumstances as these would put other children and staff at risk. Year 6 children, who walk home after school, may leave a mobile phone at the school office and collect it at the end of the day.

As a school, we educate our children about how to use technology safely. We follow the Google Be Internet Legends scheme of work to support this so that children are taught to identify potential dangers and are taught how to respond to threats or concerns in the appropriate manner. The children also share a wide range of learning opportunities using online platforms such as Scholastic Reading Pro, Times Table Rock stars, LBQ and Google Classroom- these applications enable the children to exchange work and share ideas with their peers. They are used in complete supervision to ensure the safety of all.

All staff evaluate websites prior to their use in a lesson and before being shared with pupils. An embedded or previously used weblink will be checked for suitability due to the regular changing and updating of a website's content to ensure it remains suitable. All staff pay particular attention to avoiding YouTube videos with advertisements and use concise clips where possible. Where possible, staff will choose videos where comments have been disabled.

At Cannon Park Primary School we teach children how to engage safely with the internet and how to protect themselves online. As part of our curriculum, our children will:

- Challenge information and consider the integrity of its source including manipulated or edited material such as AI generated content
- Be taught that not all sources on the internet are correct or useful.
- Be taught to recognise common social media and internet-based scams.
- Understand that some websites may have hidden agendas.
- Learn why It is important to remain anonymous online.
- Protect their online image by careful vetting of images and text.
- Recognise that information shared online has a footprint and cannot be undone.
- Learn that misunderstandings can occur when communicating electronically.
- Know how to protect themselves.
- Know how to confidently report cyber bullying to a trusted adult.
- Support their peers in making smart online decisions and referring them to a grown up where required.

They are confident in discovering new things:

- Look for ways to use new technologies, to present work, share information and communicate effectively.
- Evaluate new technologies considering the benefits, disadvantages and the safety risks.

They evaluate risks in technology:

- Weigh up possible and likely dangers, particularly applicable for unmoderated chat rooms and social networking sites.
- An understanding of how to reduce the risks involved when using online tools for communication, for example, allowing real world friends only.
- To understand the risk of sharing passwords and usernames.
- Be aware of anti-virus software and its purpose.
- Know that not all emails are trustworthy and that they should only open an email if they trust the source.

Evaluate internet content:

Online Safety lessons are incorporated into the computing and PSHE curriculum. All staff have a responsibility to educate children on both the risks and benefits of the internet during Computing and PSHE sessions and where relevant when assessing the needs of the class – during anti-bullying week, healthy schools week and Online Safety Day.

The use of E-mail:

Pupils use a secure email account hosted by Cannon Park Primary School to enable them to access G-Suite, the Google Classroom and its partner apps whilst at school and at home. Children do not access email communication with their school email addresses but are able to comment on their own and others work when using the Google Classroom and whilst under the supervision by the classroom teacher.

Social network:

The LA currently controls access to social networking sites by using Smooth wall filtering and are therefore not available for pupils use within school. Pupils are advised never to give out personal details of any kind which may identify them, their friends or their location. Lessons regarding the appropriateness and risks of social networking are taught during computing and PSHE lessons.

Monitoring internet usage:

Our broadband internet connection is provided by Coventry City Council and incorporates a filtering system which is appropriate to the age of our pupils. Undesirable sites are blocked by a proxy server. Any concerns over a website will be reported to the ICT Manager and the LA will be informed so that necessary changes are made to the filtering system. ICT used by staff is protected by antivirus software and is monitored regularly. The head teacher ensures that technology is used safely throughout the school via Impero which informs him of potential misuse. This is checked termly by the Chair of Governors.

Addressing concerns:

Misuse of the Internet will not be tolerated at Cannon Park. The class teacher will formally report any misuse, informing safe guarding leads and parents where required and report every incident via CPOMs. The sanctions imposed will reflect the severity of the incident and will follow the school's behaviour policy. Pupils must report accidental access or inappropriate material immediately to their teacher, who will then inform the ICT manager and/or Coventry City Council.