Cabot Primary School

Learn together, respect each other, achieve forever

Cabot Primary School

Online Safety Policy

This policy should be read alongside Cabot Primary School's policies and procedures on child protection and safeguarding. More information about safeguarding and child protection can be found at learning.nspcc.org.uk/key-topics/safeguarding-and-child-protection.

Review Date	Details	Owned by/linked to
November 2017	New Policy	School (SIC)
November 2019		
February 2021	New Policy	School (SIC)
February 2023		

Designated online safety co-ordinator: Tom Burton

ICT Leader: Mel Codling

Safeguarding Governor: Dan Watkins

Technical Staff (TWSIT): David Meek

School Context

Cabot Primary School works with children and families as part of its activities. Cabot is a successful, high achieving primary school located in the heart of St Pauls, Bristol. It is a diverse and vibrant community with a rich and proud history.

Our core values reflect our belief that education is often collaborative, based on great relationships and should prepare children for life. It underpins everything we do at Cabot.

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.
- The policy statement applies to all staff, volunteers, children and young people and anyone involved in Cabot Primary School's activities.

Legal framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:

- online abuse learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse
- bullying learning.nspcc.org.uk/child-abuse-and-neglect/bullying
- child protection learning.nspcc.org.uk/child-protection-system

We believe that:

- children and young people should never experience abuse of any kind
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- the online world provides everyone with many opportunities; however it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people safe online, whether or not they are using Cabot Primary School's network and devices
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse

- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

We will seek to keep children and young people safe by:

- appointing an online safety coordinator, This will be a Designated Safeguarding Lead. Together with the ICT Leader, the will oversee day to day responsibilities
- providing clear and specific directions to staff and volunteers on how to behave online through the Staff Code of Conduct adults
- supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- supporting and encouraging parents and carers to do what they can to keep their children safe online
- developing an online safety agreement for use with young people and their parents/carers (see Acceptable Use Agreement, appendix 1)
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person (See Safeguarding Policy for incident reporting procedures)
- reviewing and updating the security of our information systems regularly
- ensuring that usernames, logins, email accounts and passwords are used effectively
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse, including online abuse (See Safeguarding Policy for incident reporting procedures)
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. The monitoring of the implementation of the Online Safety Policy will be included in the role of the named governor for Child Protection and Safeguarding.

- monitoring of online safety incident logs
- reporting to Resources Committee

Headteacher and Senior Leaders:

- The Headteacher *has* a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to all teaching and learning staff.
- The Headteacher and Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (The Headteacher and Senior Leaders are responsible for ensuring that the ICT Leader and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. TWSIT provides school with a fully managed Internet Services the details of which can be found here: http://ict.tradingwithschools.org/internet-services-service-detail/

- The Senior Leadership Team will receive regular monitoring reports from the ICT Leader.

ICT Leader:

- leads the Online Safety issues within the Safeguarding Team
- oversees the day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

TWS IT are employed to manage the technical service provided to the school.
TWS IT provide technical staff who are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (This is done through TWS IT services)
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- that the use of the network, internet and remote access is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher or IT Leader for investigation.
- that monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Code of Conduct
- they report any suspected misuse or problem to the Headteacher, Senior Leadership Team or IT Leader for investigation and action
- Online Safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, where possible, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parent sessions, policies, home-school agreements, newsletters and information about national or local online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of digital and video images taken in school.

Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

- Child protection
- Procedures for responding to concerns about a child or young person's wellbeing
- Dealing with allegations of abuse made against a child or young person
- Managing allegations against staff and volunteers
- Code of conduct for staff and volunteers
- Anti-bullying policy and procedures
- Photography and image sharing guidance
- Remote Learning Policy

Appendix A
Responsible Internet Use
These rules help us to be fair to others and keep everyone safe.

- I will ask permission before using the Internet.
- I will use only my class network login and password, which is secret.
- I will only open or delete my own files.
- I must not bring into school and use software or files without permission.
- I will only e-mail and open attachments from people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I understand that the school may check my computer files, e-mails I send and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Cabot Primary School

Acceptable Use of the Internet Agreement

Please sign and return the form below:

Pupil:	Class:
Pupil's Agreement I have read and I understand the school rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and follow these rules at all times.	
Signed:	Date:
Parent's Consent for Internet Access I have read and understood the school rules for responsible Internet use and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.	
Signed:	Date: