Sutton in Craven C of E Primary School

E-Safety Policy

Date Adopted: **October 2017**
Next Review: **October 2019**
Reviewed every two years by the Improvement Committee.

Introduction

This policy has been written based on North Yorkshire e-safety guidance in conjunction with BECTA and CEOP materials. It has been adapted to reflect the schools own decisions on balancing educational benefit with potential risks. This e-safety policy will be used in conjunction with policies relating to curriculum, data protection, anti-bullying, safeguarding children, security and home-school agreements.

The Headteacher has identified **Mrs Samantha Davison** as the e-safety Co-ordinator. This policy has been prepared by the Headteahcer and e-safety co-ordinator and has been agreed by the Governing Body.

Rationale

The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning.

Aims

Internet use will support, extend and enhance learning.

- Pupils will be given clear objectives for internet use.
- Web content will be subject to age-appropriate filters.
- Internet use will be embedded in the curriculum.

Pupils will develop an understanding of the uses, importance and limitations of the internet

- Pupils will be taught how to effectively use the internet for research purposes.
- Pupils will be taught to evaluate information on the internet.
- Pupils will be taught how to report inappropriate web content.
- Pupils will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working.
- Pupils will use the internet to enhance their learning experience,
- Pupils have opportunities to engage in independent and collaborative learning using the internet and other digital technologies.
- Pupils will use existing, as well as up and coming, technologies safely.
- Pupils will be taught about e-safety.

Data Protection

There is a separate Data Protection policy.

E-mail

- Pupils and staff will only use approved e-mail accounts when using the school network.
- Pupils will tell a member of staff if they receive inappropriate e-mail communications.
- Pupils will only use e-mail for approved activities.

Internet Access

- Staff will read and sign the e-safety and acceptable use policies before using any school ICT resource.
- Pupils will be taught to use the internet responsibly and to report any inappropriate content to a responsible adult.

Mobile Phones and other handheld technology
Pupils are only permitted to have mobile phones or other personal handheld technology in school with the permission of the Headteacher. Any mobile devices brought in to school by pupils must be handed in to staff on arrical to keep secure during the school day. When pupils are using mobile technology (their own or that provided by the school) they will be required to follow the school's Acceptable Use Policy (AUP). Such items can be confiscated by school staff if they have reason to think that they are being used to compromise the wellbeing and safety of others (*Education and Inspections Act 2006, Sections 90, 91 and 94)*.

Systems Security
- ICT systems security will be regularly reviewed with support from Schools ICT.

Web Filtering
- The school will work with Schools ICT to ensure that appropriate filtering is in place.
- Pupils will report any inappropriate content accessed to their class teacher, who will alert the e-safety co-ordinator and/or Headteacher.

School Website and Published Content
- All staff who edit website content must read and sign to say they have read this policy.

Communication of the e-safety policy to pupils
- Pupils will read (or be read) and sign the age-appropriate Internet Acceptable Use Policy before using ICT resources.
- E-safety rules will be posted around the school to remind the children of these and these will be discussed regularly in lessons.
- Pupils will be informed that internet use will be monitored.
- E-safety will be included in the curriculum and regularly revisited.

Communication of the e-safety policy to staff
- The e-safety and acceptable use policies will be given to all new members of staff as part of the staff handbook.
- The e-safety and acceptable use policies will be discussed with, and signed by, all staff at least annually.
- Staff will be informed that internet use will be monitored.

Communication of the e-safety policy to parents/carers
- The acceptable use policies will be available from the school and on the school website.
- The school website will include e-safety website information for parents to access.
- The school will communicate and publicise e-safety issues to parents through meeting in school, newsletters and on the website where relevant.

E-safety Complaints
- Instances of pupil internet misuse should be reported to a member of staff.
- Staff will be trained so they are able to deal with e-Safety incidents. They must log incidents reported to them and if necessary refer the matter to a senior member of staff (the e-safety co-ordinator or Headteacher).
- Instances of staff internet misuse should be reported to, and will be dealt with by, the Headteacher.
- Pupils and parents will be informed of the consequences of internet misuse.

Whole-School Responsibilities for Internet Safety

Headteacher
- Responsible for e-safety issues within the school however day-to-day responsibility is delegated to an e-safety co-ordinator.
- Ensure that the e-safety co-ordinator is given appropriate time, support and authority to carry out their duties effectively.
- Ensure that developments at Local Authority level are communicated to the e-safety co-ordinator.

- Ensure that the Governing Body is informed of e-safety issues and policies.
- Ensure that appropriate funding is allocated to support e-safety activities throughout the school.

E-safety co-ordinator

- Primary responsibility: establish and maintain a safe ICT learning environment (under the direction of Senior Management).
- Establish and maintain a school-wide e-safety programme.
- Respond to e-safety policy breaches in an appropriate and consistent manner in line with protocols set out in policies, and maintain an incident log.
- Establish and maintain a staff professional development programme relating to E-safety.
- Develop a parental awareness strategy.
- Develop an understanding of relevant legislation and take responsibility for their professional development in this are.

Governing Body

- Support the Headteacher and/or designated e-safety co-ordinator in establishing and implementing policies, systems and procedures for ensuring a safe ICT learning environment.
- Ensure that appropriate funding is authorised for e-safety solutions, training and other activities as recommended by the Headteacher and/or designated e-safety coordinator (as part of the wider remit of the Governing Body with regards to school budgets).

Network Manager/Technical Support Staff

- Provide a technical infrastructure to support e-safety practices.
- Ensure that appropriate processes and procedures are in place for responding to the discovery of illegal materials, or suspicion that such materials are, on the school's network.
- Ensure that appropriate processes and procedures are in place for responding to the discovery of inappropriate but legal materials on the school's network.
- Develop an understanding of relevant legislation.
- Report network breaches of acceptable use of ICT facilities to the Headteacher and/or the e-safety co-ordinator.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

Teaching and Support Staff

- Contribute to the development of e-safety policies.
- Adhere to acceptable use policies.
- Take responsibility for the security of data.
- Develop an awareness of e-safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.
- Embed e-safety education regularly in the curriculum.
- Deal with e-safety issues they become aware of and know when and how to escalate them.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

Wider School Community

- This group includes: non-teaching staff; volunteers; student teachers; other adults using school internet or other technologies.
- Contribute to the development of e-safety policies.
- Adhere to acceptable use policies.
- Take responsibility for the security of data.
- Develop an awareness of e-safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.
- Know when and how to escalate e-safety issues.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

Parents and Carers

- Discuss e-safety issues with their children, support the school in its e-safety approaches and reinforce appropriate behaviours at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Model appropriate uses of new and emerging technologies.
- Liaise with the school if they suspect, or have identified, that their child is conducting risky behaviour online.
- Contribute to the development of e-safety policies.
- Read acceptable use policies and encourage their children to adhere to them.