Hemingbrough CP School

E SAFETY & INTERNET USAGE POLICY

Date of Next Review	October 2018	**Responsibility**	*Full Governing Body*
Date of Policy Adoption by Governing Body	October 2017	**Signed Ruth Waters Chair of Governors**	

This policy has been developed in conjunction with the staff and children of Hemingbrough Community Primary school. Also see the Internet Usage Staff Agreement.

The Headteacher is nominated as the e-safety co-ordinator.
This policy has been prepared by the e-safety co-ordinator and has been agreed by the Headteacher and 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.

Scope

This policy applies to all pupils, all teaching staff, all support staff, all governors and all volunteers.

Aims

Our aims are to ensure that all pupils, including those with special educational needs:

- will use the internet and other digital technologies to support, extend and enhance their learning;
- will develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world including the need to avoid undesirable material;
- will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working;
- will use existing, as well as up and coming, technologies safely.

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 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 and Learning Platform

- Staff will read and sign the *NYCC Acceptable Use Policy – ICT and e-Technology* before using any school ICT resource.
- Parents will read this policy and sign the appropriate box on the enrolment form to give consent for their child to use the internet.
- 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. 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 an appropriate member of staff.

Communication of the e-safety policy to pupils

- Pupils will read (or be read) and sign the age-appropriate Internet and Learning Platform Acceptable Use Policy before using these resources.
- E-safety rules will be posted in each room where a computer is used.
- 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.
- The e-safety and acceptable use policies will be signed by all staff and discussed with them 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 in the school prospectus and on the school website.
- The school website will include a list of e-safety resources and information for parents to access.
- Parents will be asked to sign a home-school agreement when their children join the school. This will include acceptable use policies relating to the internet, and other digital technologies.
- The school will communicate and publicise e-safety issues to parents through the school newsletter, website and Learning Platform.

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.
- 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 but may delegate the day-to-day responsibility to a Senior Leader as the 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 (ideally as part of a wider child protection role)

- 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.
- Form a school e-safety team to review and advise on e-safety policies.
- Work with the e-safety team to develop, and review, e-safety policies and procedures.
- 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.
- Form a school e-safety management team to review the effectiveness and impact of the policy.
- Establish and maintain a staff professional development programme relating to e-Safety.
- Develop a parental awareness programme.
- Develop an understanding of relevant legislation and take responsibility for their professional development in this area.

Governing Body

- Appoint an e-Safety Governor who will ensure that e-safety is included as part of the regular review of child protection and health and safety policies.
- 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 co-ordinator (as part of the wider remit of the Governing Body with regards to school budgets).
- Promote e-safety to parents and provide updates on e-safety policies within the statutory ‘security’ section of the annual report.

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.
- Include e-safety regularly in the curriculum.
- Deal with e-Safety issues they become aware of and know when and how to escalate incidents.
- 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, Learning Platform 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

- Contribute to the development of e-safety policies.
- Read acceptable use policies and encourage their children to adhere to them.
- Adhere to acceptable use policies when using the school internet and/or Learning Platform.

- 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.
- Liase with the school if they suspect, or have identified, that their child is conducting risky behaviour online.

e-Safety Rules agreed by our children

- Make security settings really high
- Get someone to check a website is suitable
- Don't open messages if you don't know who they are from
- Don't send or open viruses
- If you see something suspicious tell an adult
- Make sure you shut down and turn off
- Always ask an adult before downloading a game
- Check typing is done properly
- Don't click on things to buy things
- Read things carefully
- Make sure an adult knows you are on a device
- Don't tell other people your password
- Keep your phone safe!
- Never play against someone you don't know
- If you get a mean message tell an adult