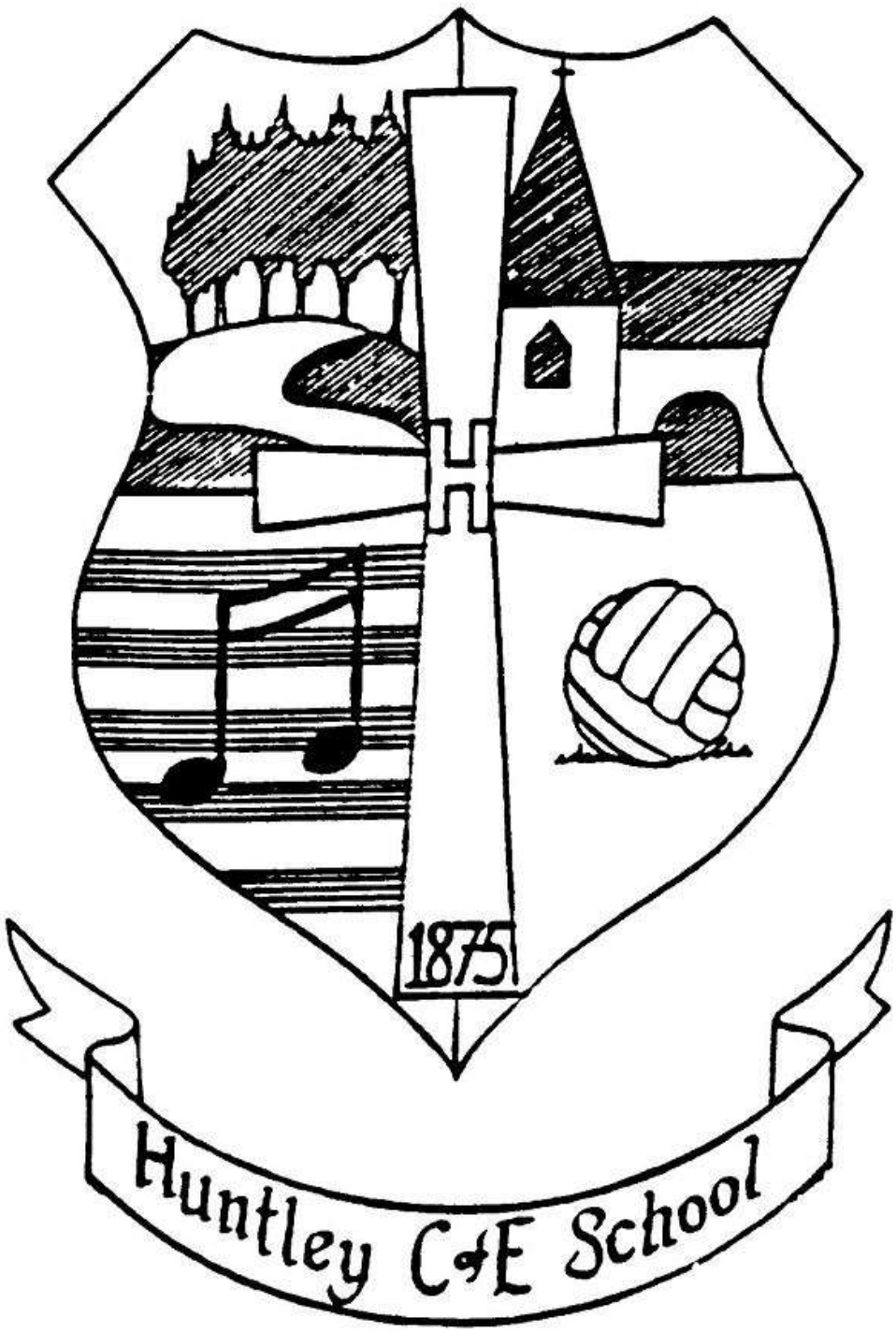

E-SAFETY POLICY

Spring 2016

Reviewed annually

To read in conjunction with our
Safeguarding Child Protection Policy

Rationale for a School e-Safety Policy

The Internet can be used by pupils of all ages, by teachers and by managers. Home Internet use is becoming an important part of learning and communication during leisure time.

However, the Internet is managed by a world-wide collaboration of independent agencies and serves mainly an adult audience. Without appropriate measures, access to unsuitable materials would be possible and security compromised. An Internet Access Policy will help to ensure that Internet use supports schools' educational aims, that responsibilities to pupils are met and that School requirements are satisfied.

Who will write and review the policy?

- Our e-Safety Policy has been written by the ICT Subject Leader and Headteacher, building on the government guidance. It has been agreed by the senior management and approved by governors and staff.
- The e-Safety Policy will be reviewed annually.
- The full policy will be available for staff, governors, children and parents both in school and on the school's website.

Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils It should be noted that the use of a computer system without permission or for a purpose not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does the Internet benefit education?

A number of studies and government projects have indicated the benefits to be gained through the appropriate use of the Internet in education.

These benefits include:

- Access to world-wide educational resources including museums and art galleries
- Inclusion in the National Education Network which connects all UK schools
- News and current events
- Cultural, vocational, social and leisure use in libraries, clubs and at home

- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice
- Collaboration with support services, professional associations and colleagues
- Improved access to technical support including remote management of networks and automatic system updates
- Exchange of curriculum and administration data with the LA (Local Authority) and DfE
- Access to learning wherever and whenever convenient

How can the Internet enhance learning?

- The school Internet access is designed for pupil use and includes filtering appropriate to the age of pupils
- Pupils have been taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and ability
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

How will pupils learn how to evaluate Internet content?

- All children will be aware of children's Rights and Responsibilities. The use of a school e-safety charter ensures that all children are able to follow an agreed set of steps which supports their learning but helps to protect them in relation to dangers of the internet. The charter is visual in all classrooms and in all learning areas where children may have access to online activities via computers or laptops (See Appendix 1 – SMART Rules).
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Internet Service Provider via the ICT coordinator Gail Bennett.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law
- Pupils should be taught to be aware of the materials they read and shown how to validate information before accepting its accuracy
- The evaluation of on-line materials is a part of every subject

- Pupils will be made aware that the writer of an E-mail or the author of a Web page may not be the person claimed
- Pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV
- Pupils will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable

How will ICT system security be maintained?

- The security of the school ICT systems will be reviewed regularly
- Virus protection will be installed and updated regularly
- Personal data sent over the Internet will be encrypted or otherwise secured
- Use of portable media will be reviewed. Portable media may not used without specific permission and a virus check
- Files held on the school's network will be regularly checked
- The IT co-ordinator will review system capacity regularly

How will e-mail be managed?

- Pupils may only use approved e-mail accounts on the school system
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Whole-class or group e-mail addresses should be used. The children will not have individual email address but use an email address for their year group within their current class. An example of an address for these emails is; *year4@huntley.gloucs.sch.uk* (this being the email address for year 4 children)
- Access in school to external personal e-mail accounts may be blocked
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- The forwarding of chain letters is not permitted

How will published content be managed?

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published
- Email addresses should be published carefully, to avoid spam harvesting
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright

Can pupil's images or work be published?

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (see Appendix 2 - Acceptable Internet Use Policy)
- Pupil's work can only be published with the permission of the pupil and parents. Written consent will be obtained from children's parent or guardian (see Appendix 2 - Acceptable Internet Use Policy)

How will social networking and personal publishing be managed?

- The school will block/filter access to social networking sites
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, e-mail address, names of friends, specific interests and clubs etc
- Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. House number, street name, school, shopping centre.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others
- Pupils should be advised not to publish specific and detailed private thoughts
- We are aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments
- **We need to be aware of signs children maybe accessing content considered to be radical such as increased instances of**
  - A conviction that their religion, culture or beliefs are under threat and treated unjustly
  - A tendency to look for conspiracy theories and distrust of mainstream media
  - The need for identity and belonging
  - Being secretive about who they have been talking to online and what sites they visit
  - Switching screens if someone comes near device
  - Possessing items not given to them by parents
  - Becoming emotionally volatile

What can lead children to become radicalised?
Political and religious groups can provide a sense of family or support that children may feel is lacking in their lives. This desire for security could also be due to poverty, social isolation or feelings of rejection by their own faith, family or social circle.
In some cases the trigger may be an event, either global or personal, such as being a victim or witness to a race or religious hate crime. It maybe as a result of peer pressure and the desire to 'fit in' with their social circle.
However, it should be remembered that not all children that experience these factors adopt radical views.

Referral Process
Staff and visitors to the school must refer all concerns about pupils who show signs of vulnerability or radicalisation to the Designated Safeguarding Lead. This in turn may be referred to the appropriate body.

How will filtering be managed?

- We will work in partnership with parents, the LA, Department for children, schools and families (previously DfES) and the Internet Service Provider (SWGfL) to ensure systems to protect pupils are reviewed and improved
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Internet Service Provider. Children will be educated as to the correct and safe procedure to do this
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (www.iwf.org.uk)
- Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate

How can emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed
- Staff will be issued with a school phone where contact with pupils is required

How should personal data be protected?

The Data Protection Act 1998 requires that data is**:**

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individuals rights

- Kept secure
- Transferred only to other countries with suitable security measures

How will Internet access be authorised?

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn (See Appendix 3 – Template for Internet Permission)
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- At Key Stage 2, access to the Internet will be through the same channels but with more opportunities for the children to work directly on the Internet individually or with a partner. This will always be directly supervised by a teacher or adult
- Parents will be informed that pupils will be provided with supervised Internet access
- Parents will be asked to sign and return a consent form (See Appendix 2 - Acceptable Use Policy)
- Primary pupils will not be issued individual e-mail accounts, but will be authorised to us a group/class email address under supervision

How will risks be assessed?

- 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 a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990
- Methods to identify, assess and minimise risks will be reviewed regularly
- The headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored

How will e-safety complaints be handled?

Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance it is possible that the issue has arisen through home Internet use or by contacts outside school. Transgressions of the rules by pupils could include minor as well as the potentially serious. Sanctions for irresponsible use will be linked to the school's Behaviour and Discipline Policy.

- Complaints of Internet misuse will be dealt with by a senior member of staff

- Any complaint about staff misuse must be referred to the headteacher
- Pupils and parents will be informed of the complaints procedure
- Parents and pupils will need to work in partnership with staff to resolve issues
- Discussions will be held with the Police liaison officer to establish procedures for handling potentially illegal issues
- Sanctions within the school discipline policy include:
    - interview/counselling by teacher/headteacher
    - informing parents or carers;
    - removal of Internet or computer access for a period of time

How is the Internet used across the community?

- The school will liaise with local organisations to establish a common approach to e-safety
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice

How will the policy be introduced to pupils?

- Rules for safe Internet access will be posted in all areas of the school with access to the internet (See Appendix 2 - Acceptable Use Policy). These rules will be carefully written and illustrated to ensure all children understand their message. Children from the School Council will be involved to ensure these rules are approved by children, for children
- Pupils will be informed that Internet use will be monitored
- An e-Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede Internet access. When this policy is released to pupils, staff, parents, the internet will be out of bounds until consent has been received
- A module on responsible Internet use will be included in the ICT programme covering both school and home use

How will the policy be discussed with staff?

- All staff must accept the terms of the 'Acceptable Use Policy' (See Appendix 2 - Acceptable Use Policy) statement before using any Internet resource in school
- All staff will be given the School e-Safety Policy and its importance explained to them. The whole staff will also be involved in the confirmation of the final draft of this policy before release to parents and children
- Staff will be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential

- The monitoring of Internet use is a sensitive matter. Staff that operate monitoring procedures should be supervised by senior management and members of the e-safety committee

- Staff development in safe and acceptable use of the Internet and on the school e-Safety Policy will be provided as required

How will parents' support be enlisted?

- Parents' attention will be drawn to the School e-Safety Policy in initial letters and newsletters and from then onwards; the school brochure and on the school website

- Internet issues will be handled sensitively to inform parents without alarm
- A partnership approach with parents will be encouraged. This includes parent Internet safety information evenings which would include demonstrations, practical activities and suggestions for safe home Internet use

- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents