HANNAH MORE
PRIMARY SCHOOL

Policy Title: E-Safety Policy

Date Drafted: 01.2012

Date Ratified by Governors:

Effective From:

Date for Renewal:

Signed by the Headteacher:

Policy Structure:

1. *Rationale*
2. *Guided Educational Use*
3. *Risk Assessment*
4. *Responsibility*
5. *Regulation*
6. *Appropriate Strategies*
7. *Guidelines for Internet Use and Learning*
8. *Authorisation of Access*
9. *Management of Filtering*
10. *Risk Assessment*
11. *Evaluating Content*
12. *Managing School Website Content*
13. *Managing Communication Technologies*
14. *Introducing the policy to pupils, parents and staff*
15. *Complaints Procedure*

1. Rationale

The internet is now regarded as an essential resource to support teaching and learning. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail. Schools are ideally placed to help young people learn to become E-safe.

The internet is becoming as commonplace as the telephone or television and its effective use is an essential life-skill. Unmediated internet access brings with it the possibility of placing of pupils in embarrassing, inappropriate and even dangerous situations. Hannah More Primary's E-Safety Policy is built on the following five core principles:

- Guided educational use
- Risk assessment
- Responsibility
- Regulation
- Appropriate strategies

2. Guided educational use

Significant educational benefits should result from curriculum internet use including access to information from around the world and the ability to communicate widely and to publish easily. Curriculum internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful internet use will also reduce the opportunities for activities of dubious worth.

3. Risk assessment

21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they must learn to recognise and avoid these risks – to become 'internet wise'. As a school we need to ensure that they are fully aware of the risks and pupils need to know how to cope if they come across inappropriate material.

4. Responsibility

Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of internet and other communication technologies such as mobile phones.

5. Regulation

Fair rules, clarified by discussion and prominently displayed at the point of access will help pupils make responsible decisions. In some cases, access must simply be denied. For instance, un-moderated chat rooms present immediate dangers and are banned.

6. Appropriate strategies

This document describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding pupils towards educational activities. There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

7. Guidelines for internet use and learning

It is now common place to see computers and the internet being used regularly both in school and at home, it is therefore important that children become 'web literate' knowing the importance of keeping personal information safe and know that all they see on the internet may not be as it seems.

- The purpose of internet use in school is to raise educational standards, to promote pupil achievement, wellbeing and to support the professional work of staff. Enhance the school's information management and business administration systems.

- The school internet access is designed expressly for educational use and includes filtering appropriate to the age of pupils.

- The use of the internet is a part of the statutory curriculum and a necessary tool for staff and pupils.

8. Authorisation of access

- 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.

- Primary pupils will not be issued individual email accounts .

- At Key Stage 1, access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials.

- Parents will be informed that pupils will be provided with supervised internet access

- During induction to the school parents will be asked for permission to allow their children to access the internet at school.

- Children will not be allowed to access the internet without adult supervision

9. Management of filtering

• The school will work in partnership with parents, Bristol County Council and the SWGfL to ensure systems to protect pupils are reviewed and improved.

• If staff or pupils discover unsuitable sites, the URL (address) and content must be reported by the designated member of staff and then to the internet Service Provider by;

Phone: 0117 9037999 email: cyps.it.helpdesk@bristol.gov.uk

Or

abuse@swfl.org.uk

• The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

10. Risk assessment

- 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. Neither the school nor Bristol County Council can 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 internet policy is implemented and compliance with the policy monitored.

11. Evaluating content

- Hannah More will ensure that the use of internet derived materials by staff and by pupils complies with copyright law.
- Specific lessons will be included within the ICT Scheme of Work that teaches all pupils how to read for information from web resources. For example lesson plans from www.thinkyouknow.co.uk. Other topics may be covered within different areas of learning. For example Cyber bullying could form part of anti-bullying week.

- A nominated person will be responsible for permitting and denying additional websites as requested by colleagues.
- When using internet research in class work, KS2 learners will be taught to acknowledge the source of information used.

12. Managing school website content

- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission will gained from parents or carers during induction to the school to allow photographs of pupils to be published on the school website.
- The designated person will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

13. Managing communication technologies

- Pupils may only use approved internal e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.
- Pupils should use email in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of school conduct and will be dealt with accordingly.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and will not be permitted.
- Students/pupils will be taught about how to keep personal information safe when using online services. Each year group will have specific ICT lessons dedicated to e-safety.
- The use of online chat is not permitted in school, other than as part of its online learning environment.

- Information is regularly shared via newsletters regarding the safe use of the internet at home and where specific cases of poor use are brought to the attention of the school letters are sent home and parents contacted as appropriate.
- Mobile phones are not permitted within the school. Pupils will be asked to give them to the office at the start of the school day. Any pupil not handing in a phone is at risk of having it confiscated.

14. Introducing the policy to pupils, parents and staff

- Rules for internet access will be posted in all rooms where computers are used.
- Instruction on responsible and safe use should precede internet access in the form a guidance lessons at the start of a school year.
- Pupils will be informed that internet use will be monitored.
- Parents' attention will be drawn to the School E-Safety Policy in newsletters and on the school Website.
- Regular information will be provided to parents about how to ensure they can work with the school so that this resource is used appropriately both within school and home.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- Interested parents will be referred to organisations such as PIN, Parents Online and NCH Action for Children
- All staff including teachers, supply staff, classroom assistants and support staff, will have access to the School E-safety Policy.
- The school's consequences for internet and mobile phone misuse will be clear so that all teachers are confident to apply this should the situation arise.
- All staff must accept the terms of the 'Laptops for teachers –Acknowledgement' statement before using any internet resource in school.
- Discretion and professional conduct is essential.

15. Complaints procedure

- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils of Hannah More Primary School will need to work in partnership with staff to resolve issues.

- As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
- Sanctions available include:
    - Informing parents or carers.
    - Removal of internet or computer access for a period, which could ultimately prevent access to files held on the system.