*C*aring *A*chieving *R*espectful *E*xciting

E-Safety Policy

School Leader: **G Nowak**

Link Governor: **C Foyle**

Policy Approved	**Signed: J Robinson**	**Date: 08.06.17**
Policy Reviewed	Signed: J Robinson	Date: 07.06.18
Policy Reviewed	Signed: C Foyle	Date: 20.06.19
Policy Reviewed	Signed: C Foyle	Date: 18.06.2020
Policy Reviewed	Signed:	Date:

Content

1.   The importance of Internet and digital communications

- The purpose of Internet and digital communication use in school are 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, digital media and digital communication use are part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for all pupils.
- The Internet and digital communications are an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide students with quality Internet and digital communications access as part of their learning experience.

2.   Teaching and learning

Benefits of the internet and digital communication in education

Benefits of using the Internet in education include:
- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks.

How the Internet and digital communications will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what is acceptable and what is not acceptable 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 maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval.
- Pupils will be shown how to publish and present information to a wider audience.

Pupils will learn to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.
- Training will be made available to all staff in the evaluation of Web materials and methods of developing students' critical attitudes.
- Pupils will be taught how to report materials that they feel are distasteful, uncomfortable, unpleasant or threatening to an adult.

3. **Managing internet access**

   Managing e-mail / internal messaging system (Purple Mash)

- Pupils may only use approved e-mail / message accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail/ message.
- Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail / message communication.
- Pupils must agree to abide by the acceptable use agreement when using their email / message account.
- E-mail \ message 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 banned.
- Pupil email / message accounts will be restricted as appropriate.
- Pupils will be taught the importance of keeping their passwords private.

   Managing 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.
- Website photographs that include pupils will be selected carefully and will not enable individual pupils to be identified.
- Pupil image file names will not refer to the pupil by name.
- Pupils' full names will not be used anywhere on the Website, particularly associated with photographs.
- Written permission from parents will be sought before photographs of pupils are published on the school Website.
- The headteacher or nominee will take overall editorial responsibility and ensure 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.

Managing social networking and personal publishing

- Pupils will not be allowed access to public or unregulated chat rooms.
- Children should use only regulated educational chat environments. This use will always be supervised and the importance of chat room safety emphasised.
- Newsgroups will not be made available unless an educational requirement for their use has been demonstrated.
- Pupils will be advised not to give out any personal information that could identify themselves, their school or their friends.
- Pupils will be advised on the use of avatars and nicknames when using any kind of chat or social networking site.
- Parents and pupils will be advised of dangers that social network spaces outside of school bring and how to stay safe.

Managing filtering

- The school will work in partnership with parents, the LA, DDAT, DfEE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate and effective.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (see appendix).
- If staff or students require an alternative filtering strategy, an assessment will be made and a new filtering profile designed, where appropriate.

Managing webcam and videoconferencing

- Use of webcams and videoconferencing must be supervised.
- Appropriate permissions must be obtained.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- School leaders need to have an awareness that new mobile wireless internet technology could bypass school filtering and leave pupils open to inappropriate content.

Authorising Internet, and email access

- The school will keep a record of all staff and pupils with email accounts. The record will be kept up-to-date, for instance a member of staff leaving or the withdrawal of a pupil's access.
- Pupils will be taught not to share their password with others.
- At Key Stage 1, access to the Internet will be by adult demonstration with supervised access to specific, approved on-line materials.

Assessing the risks

- 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 DDAT 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.

4.   **Communicating the policy**

Introducing the policy to pupils

- Rules for Internet access will be discussed with the children so that they are fully understood.
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- Safe and responsible use of technology will be embedded in the PSHE curriculum.
- E-safety will be included as part of the Scheme of Work for Computing (Purple Mash).

E-safety policy and parents

- Parents' attention will be drawn to the School Internet Policy in newsletters, the school brochure and on the school website.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

The e-safety policy and staff

- All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.
- All staff must read, agree to and sign the ICT acceptable use policy.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the e-Safety Policy, and its importance explained.
- Staff should 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 who operate monitoring procedures should be supervised by senior management.
- Staff development in the safe and responsible Internet use and on school Internet policy will be provided as required.

5. Maintaining ICT system security

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the DDAT, particularly where a wide area network connection is being planned.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Use of disks and other portable data storage devices will be reviewed. Personal portable data storage devices may not be brought into school and used without specific permission and a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.
- The network manager will ensure that the system has the capacity to take increased traffic caused by Internet use.

6. Handling complaints regarding Internet use

- Responsibility for handling incidents will be delegated to 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.
- Sanctions may need to be applied. These include:
  - interview/counselling by headteacher;
  - informing parents or carers;
  - removal of Internet or computer access for a period, which could prevent access to school work held on the system.

7. Appendix 1
See following page
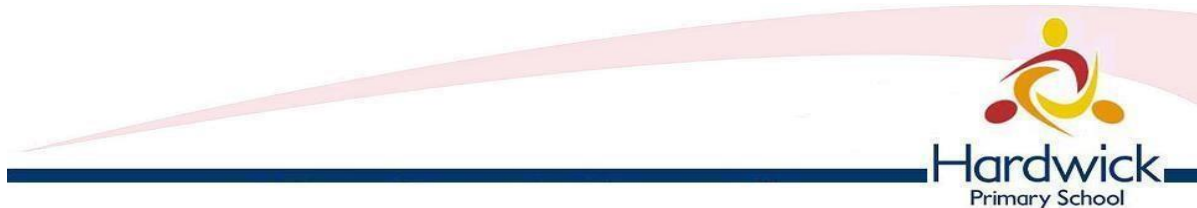
Responsible Internet and Purple Mash Use

Pupil agreement

• I will ask permission before entering any website, unless my teacher has already approved that site.
• On a network, I will use only my own login and password, which I will keep secret. I will always logout when I have finished using the computer.
• I will not look at or delete other people's files.
• I will not bring memory sticks into school without permission.
• I will only send messages to people I know, or my teacher has approved.
• The messages I send will be polite and sensible.
• When sending messages, I will not give my home address or phone number, or arrange to meet someone.
• I will ask for permission before opening a message or an attachment sent by someone I do not know.
• If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
• I know that the school may check my computer files and may monitor the Internet sites I visit.
• I understand that if I deliberately break these rules, I could be stopped from using email or internet.

 I agree to follow these rules for internet, email and learning platform use.

Name:_____

Signed: _____   Date:_____

Parent/Carer Agreement

• I have read and understood the internet and email use agreement signed by my child and will enforce these rules at home when my child uses his/her Purple Mash account outside of school.
• I will not give my child's logon details or password to anyone else. I will ensure that my child logs out at the end of the session.
• I will not use my child's Purple Mash account to send messages personally or on behalf of my child.

 I have read and understood the above. I agree to abide by the above agreement.

Name:_____   (parent/guardian)

Signed:_____   Date:_____
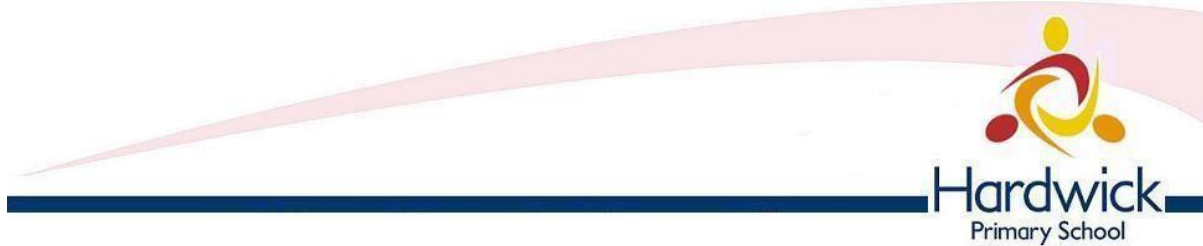
Dear Parents

Responsible Internet Use

As part of your child's curriculum and the development of Computing skills, our school is providing supervised access to the Internet. We believe that the use of the Web and Purple Mash is worthwhile and an essential tool for children as they grow up in the modern world. Please read the rules and agreements for responsible Internet and email use. Then sign and return the agreement.

Although there have been concerns about pupils having access to undesirable materials, we are taking positive steps to deal with this risk in school. Our school Internet access provider operates a filtering system that restricts access to inappropriate materials. This may not be the case at home and we enclose references to information on safe Internet access that may be of use.

Whilst every effort is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable under any circumstances for any damages arising from your child's use of the Internet facilities. I enclose a copy of the rules for Responsible Internet Use that we operate at our school. We also have a number of leaflets from national bodies that explain issues further.

Should you wish to discuss any aspect of Internet use please telephone the office to arrange an appointment.

Yours sincerely,

R Sandhu
Head of School

References

Particularly for Parents

National Action for Children (NCH) https://www.actionforchildren.org.uk/
Parents' Guide on Internet usage Current activities to promote safe use

Internet Watch Foundation www.iwf.org.uk **-** report inappropriate Web sites
Safe Surfing Guide for parents and carers:
Which article on Internet filtering for home use

Parents Information Network (PIN) http://pin.bamsi.org/
Comprehensive guidelines on Internet safety

Particularly for Schools

The South West Grid for Learning http://swgfl.org.uk/
A leading organisation that supports schools and other organisations in safeguarding
children online.
British Computer Society
http://www.bcs.org/category/5651 A guide for schools
prepared by the BCS Schools Committee
and the National Association of Advisers for Computer Education (NAACE)

Internet Watch Foundation www.iwf.org.uk
Invites users to report illegal Web sites

SEGfL ICT Security Policy http://swgfl.org.uk/products-services/online-
safety/resources/online-safety-policy-templates An overview of the security of networks
with Internet access.