

Learning together to be
the best we can be.....

Headteacher – Nichola Irving



E-Safety Policy

Safeguarding Statement

Everyone at Horton Grange shares an objective to help keep children and young people safe by contributing to:

- Providing a safe environment for children and young people to learn in school and;
- Identifying children and young people who are suffering or likely to suffer significant harm, and taking appropriate action with the aim of making sure they are kept safe both at home and in school.

Reviewed: July 2017
Next review: Sept 20

Learning together to be the best we can be.....

Headteacher – Nichola Irving



Introduction

Writing and reviewing the e-safety policy

The e-Safety Policy is part on going school improvement and relates to other policies including those for ICT, digital imagery, anti-bullying and for child protection.

- Our e-Safety Policy has been written by the school, building on the Kent e-Safety Policy and government guidance. The e-Safety Policy and its implementation will be reviewed annually.

E-Safety Co-ordinator: Hamish Fields (ICT Co-ordinator)

E – Safety Lead: Emma Brownrigg

Designated Senior Person for Child Protection: Nichola Irving (Headteacher),

1.1 Why the Internet and digital communications are important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

1.2 Internet use will enhance learning

The school's curriculum ICT system is monitored by PCE which sends weekly updates to the E-Safety co-ordinator regarding unacceptable use of the system. This identifies individual pupils, staff or computers which have been used and reports on the types of inappropriate access. This can then be managed according to the school's behaviour policy.

Virus protection is updated regularly.

Staff are not permitted to access the school's wireless technology with their personal laptops unless PCE is installed.

Staff using school laptops at home are aware that PCE is installed on all units and that the appropriate use of the equipment will be monitored when the laptop accesses the school's wireless system on its return to school

All internet access including e-mails will be monitored through PCE on the curriculum network. The admin system is protected by a separate firewall system.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be shown how to publish and present information to a wider audience and how to evaluate Internet content.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Learning together to be the best we can be.....

Headteacher – Nichola Irving



Pupils will be taught the importance of cross-checking information before accepting its accuracy and how to report unpleasant Internet content e.g. Hector Protector

2. Managing Internet Access

2.1 Information system security

- School ICT systems security will be reviewed regularly following guidance from NCC exemplar policies.
- Virus protection will be updated regularly through automatic updates.
- Passwords and network/MIS/school email user names will be kept safe and secure.

2.2 E-mail

- Pupils may only use approved e-mail systems which are safe, secure and monitored by staff.
- Staff are issued with google gmail accounts.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.

2.3 Published content and the school web site

- Staff or pupil personal contact information will not be published.
- The headteacher / DHT will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.4 Publishing pupil's images and work

- Parents sign an authorisation form when their child begins Horton Grange Primary, giving permission for images of their child (or their work) to be used on the website and on other publications e.g. weekly newsletter. Where this permission is not granted, photos/work are never used.
- Photographs that include pupils will be selected appropriately to avoid images being misused. Although pupils may be recognised, photos used on the website are low-quality, and if required, edited to prevent children without photographic consent to be identified. Ref; Policy for Safeguarding Board. Guidance on use of pupil images.
- Only pupils' first names will be used on the school website or other on-line space in association with photographs or video, unless express permission has been granted by parents/carers (refer to photograph/image consent form – Appendix 1)
- Special written permission from parents or carers will be obtained before images of pupils are published anywhere other than the school website (e.g. local newspapers, outside agencies, CVTV)
- Images on shared drive and not on individual computers.

Learning together to be the best we can be.....

Headteacher – Nichola Irving



2.5 Social networking and personal publishing (e.g. blogging)

- Pupils are advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

3. Managing filtering

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the E-Safety Co-ordinator. Sites can be referred to the Helpdesk team on 01670 35555 for global blocking.
- Policy Central logs will be eventually monitored by the DHT / Headteacher.

4. Managing emerging technologies

Emerging technologies are evolving at a rapid rate and although every attempt is made to protect children from offensive or inappropriate material and misuse, there may be occasions when inadvertent access occurs.

The following points apply;

If staff or pupils discover an unsuitable site, it must be reported immediately to the teacher and then the E-Safety co-ordinator, who will report the site to the appropriate person in the Local authority (John Devlin) to ensure that the site is blocked. If it is felt that the incident is a child protection issue, the flow chart for reporting this will immediately be put into place.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications. Pupils at Horton Grange Primary are not usually permitted to have mobile phones in school and in emergency circumstances where they do need to be in contact with parents/carers before or after school, pupil phones are held securely in the school safe during the school day.
- Games machines including the Sony Playstation, Microsoft Xbox and others may have games that are age-inappropriate. Care is required in any use in school and must be supervised by staff.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school. E.g. Schools 360

4.1 Use of iPads

iPads and other mobile learning technologies are becoming an essential part of learning at Horton Grange. Every year group has been provided with ipads by the school for use

Learning together to be the best we can be.....

Headteacher – Nichola Irving



in lessons and other educational activities.

All apps will be purchased and allocated by the IT team, in consultation with teaching staff.

Pupil access to iPads will be monitored in school and use of the internet, as with all web-enabled technology, will be supervised.

4.2 Staff Use of personal Mobile Phones/cameras/ipads

- Staff may be required to take personal mobile phones on trips. These must not be used to capture images of pupils, and ideally, should not be used to make contact with parents or pupils. Emergency calls, where necessary should go through the school office.
- School digital cameras / ipads are provided. Where personal digital cameras are used in school, images should be downloaded in school, and memory cards formatted before and after use. Where possible, school-owned memory cards should be used in personal cameras and must be used solely for school purposes.

4.3 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998
- When PC / laptops are left they must be locked

5. Policy Decisions

5.1 Authorising Internet access

- All staff must read and sign the Staff AUP. All children and parents are requested to sign age appropriate AUP.
- At Key Stage 1, access to the Internet will be by adult demonstration with supervised access to specific, approved on-line materials.
- Children are required to read and accept age appropriate AUP guidelines when logging onto a computer.
- Any person not directly employed by the school will be asked to accept the AUP before being allowed to access the internet from the school site.
- All users of the school computer system understand that the systems in place afford no privacy.

5.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Northumberland LA will do as much as possible to prevent access to inappropriate material.
- The school will audit ICT use on a regular basis to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective through informal/formal monitoring and eventually the use of Policy Central.

Learning together to be the best we can be.....

Headteacher – Nichola Irving



5.3 Handling e-safety complaints

- 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.
- Complaints of a child protection nature must be dealt with in accordance with school and LA Child Protection Procedures.
- If a serious breach of the AUP is discovered, the monitor of the PC in question should be put 'out of order' but left on. This is to prevent the contamination of evidence that may be collected by outside agencies (e.g. police) if required.
- The Northumberland Safeguarding Children Board flow chart will be displayed in every room with internet access and must be followed when all e-safety incidents occur.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

6. Communications Policy

6.1 Introducing the e-safety policy to pupils

- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- E-Safety training will be embedded within the ICT scheme of work and the Personal Social and Health Education (PSHE) curriculum.

6.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff are informed that network and Internet traffic is monitored and traced to the individual user and that there should be no expectation of privacy when using any school ICT equipment (including laptops used off-site).
- Senior staff manage filtering systems and monitor ICT use in collaboration with the DSP and Headteacher.
- Staff will always use the 'safe search' facilities within search engines when accessing the web with pupils and must check all search terms before use with pupils.
- Any staff member with an online identity' (e.g. in social networking sites) will ensure that access to this information is kept private and not shared with pupils at Horton Grange Primary School. All privacy settings enabled on the account.

6.3 Enlisting parents' and carers' support

- Horton Grange Primary School's E-Safety Policy will be shared with parents and carers in the school newsletter, prospectus and school web site.
- Parents with any concerns about E-Safety are encouraged to contact the school for further guidance and support.
- Parents sign the Parent's Consent Form to allow internet access.

Learning together to be
the best we can be.....

Headteacher – Nichola Irving



Under Review

Photograph/Image Consent Form

Name of the child's
parent or carer: _____

Name of
child: _____

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make any recordings of your child for promotional purposes. Please answer questions 1 to 4 below, then sign and date the form where shown.

Please return the completed form to the school as soon as possible.

*Please circle
your answer*

1. May we use your child's photograph in printed publications that we produce for promotional purposes or on project display boards? **Yes / No**
2. May we use your child's image on our Website/Facebook/Twitter? **Yes / No**
3. May we record your child's image using digital technology? **Yes / No**
4. Are you happy for your child to appear in the media? **Yes / No?**

Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK law applies.

Please also note that the conditions for use of these photographs are on the back of this form.

I have read and understood the conditions of use on the back of this form.

Parent's or
carer's signature: _____ Date: _____

Name (in block
capitals): _____

Conditions of use

1. This form is valid for the period of time your child attends this school.
2. We will not use the personal details or full names (which means first name **and** surname) of any child or adult in a photographic image on video, on our website, in our school brochure or in any of our other printed publications without good reason. For example, we may include the full name of a pupil in a newsletter to parents if the pupil has won an award.
3. If we name a pupil in the text, we will not use a photograph of that child to accompany the article without good reason. (See point 3 above.)
4. We will not include personal e-mail or postal addresses, or telephone or fax numbers on video, on our website, in our school prospectus or in other printed publications.
5. We may include pictures of pupils and teachers that have been drawn by the pupils.
6. We may use group or class photographs or footage with very general labels, such as “a science lesson” or “making Christmas decorations”.
7. We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.

Please note that the press are exempt from the Data Protection Act and may want to include the names and personal details of children and adults in the media.

Learning together to be the best we can be.....

Headteacher – Nichola Irving



APPENDIX 2

A summary of data types and possible storage solutions

The table below does not provide guidance for every situation but provides an indication of where schools could possibly store different types of data.

| Type of data | Cloud based | | School based | Mobile | |
|-----------------------------------|----------------------|------------------------|---------------|----------------------------------|--------------------------|
| | School360 own system | School360 Google Drive | School server | Encrypted local drive Laptop/USB | Unencrypted Laptop / USB |
| Learning resources | ✓ | ✓ | ✓ | ✓ | ✓ |
| Lesson plans | ✓ | ✓ | ✓ | ✓ | ✓ |
| User created curriculum materials | ✓ | ✓ | ✓ | ✓ | ✓ |
| Pupil information, lists, d.o.b | ✓ | ✓ | ✓ | ✓ | X |
| Staff information, lists, d.o.b. | ✓ | ✓ | ✓ | ✓ | X |
| Performance management/ sickness | N/A | ✓ | ✓ | ✓ | X |
| Photographs | ✓ | ✓ | ✓ | ✓ | X |
| Behaviour reports, pupil notes | ✓ | ✓ | ✓ | ✓ | X |
| SEN Data, I.E.P'S, reports | ✓ | ✓ | ✓ | ✓ | X |
| Medical data | ✓ | ✓ | ✓ | ✓ | X |
| Assessment data | ✓ | ✓ | ✓ | ✓ | X |
| Financial | N/A | ✓ | ✓ | ✓ | X |
| Child protection | ✓ | ✓ | ✓ | ✓ | X |
| Governor information | N/A | ✓ | ✓ | ✓ | X |

Green = Recommended Amber = Consider your approach carefully Red = Not recommended.