BLACK HORSE HILL
INFANT SCHOOL

E-SAFETY (including VLE)
POLICY

Approved by Committee 28th February 2019 _____

Approved by Full Governing Body 21st March 2019 _____

Signed _____ **(Chair)**

Signed _____**(Headteacher)**

Philosophy

At Black Horse Hill Infant School, we believe that Computing expands horizons, by shrinking worlds… and with this in mind it contributes to the school curriculum in many ways:

- ♦ It prepares pupils to participate in a rapidly changing world in which work and other activities are increasingly transformed by access to varied and developing technology
- ♦ Pupils use Computing tools to find, explore, analyse, exchange and present information responsibly, creatively and within set guidelines
- ♦ Pupils learn how to employ Computing to enable rapid access to ideas and experiences from a wide range of people, communities and cultures
- ♦ Increased capability in the use of Computing promotes initiative and independent learning, with pupils being able to make informed judgements about when and where to use Computing to best effect, and to consider its implications for home and work both now and in the future

Teaching and learning

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.

Internet use 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 Internet use is acceptable and what is not and given clear objectives for Internet use.
- 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.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content.

Managing Internet Access

Information system security

- The School Computing systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.

Published content and the school web site and the VLE

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office. Any policies published on the School Website will have personal information removed e.g. Health and Safety Policy includes personal telephone numbers of Staff (Headteacher, Deputy Headteacher and Caretaker)

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. It is good practice to compress images and resize to ensure there is not mis-use.
- Pupils names will not be used on a school Web site, Twitter or other on-line space, particularly in association with photographs.
- Parents/carers will be given the right to refuse the publishing of images that include their child. This will be reviewed at the beginning of each school year. Written notice must be made and we will remind parents/carers of their right at the beginning of each year.
- Likewise if a parent/carer wishes that their child's work is not published then we will respect the parents/carers wish. Written notice must also be given.
- Parents/carers should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories. At the beginning of all school performances Parents/carers will be required to sign an agreement for the use of the images they have taken. The agreements will be kept in a file by the Headteacher.

Social networking and personal publishing

- The school will not allow access to social networking sites, but we will educate pupils in their safe use.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Photography at school performances by parents/carers, will require agreement by parents/carers in writing that no images of theirs or any other child will be published on their own personal social network site.
- Pupils and parents/carers 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.

Managing filtering

- The school will work with the Wirral LA to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator (Mr Young)
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable any issues that arise are to be reported to the Headteacher or Mrs McLeod and they will contact the school technician immediately.

Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

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.
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Pupil mobile phones are NOT permitted in school and therefore will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.
- The appropriate use of Learning Platforms or VLE will be taught in lessons and the e-safety website used to train pupils in the safe use. The appropriate use will also be shared with parents/carers.
- The VLE will not allow external messaging access. Only approved users will use the VLE and therefore will have a username and password that will not be shared by others. ***SEE VLE SECTION BELOW.***

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Virtual Learning Environments

Usage

- It is permitted that the virtual learning environment may be used within or outside of the school.
- The site is accessible through the internet and it must be acknowledged by all that use the site that this is the case.
- For security, all usage is monitored by school and therefore messages and content are logged. The acceptable use policy must be agreed before children are permitted to access the VLE.

Submitting content

Any content uploaded must not contain any of the following:

- Swearing or rude language in either censored or uncensored form.
- Slander or abuse in any form, jokingly or not.
- Rude images.
- Repeated or nuisance messages.
- Advertisement for any services, goods or events outside of the School, without being given prior permission by the Computing Management.
- Personal or private details of users.
- Content that could interfere with examination or marking.
- Viruses, ad-ware or malware of any form that could do damage to another user's iPad, laptop, PC or Mac Book.
- Anything that may offend others.

Care must be applied when posting. What qualifies any of the above in is the joint judgment of the moderators and staff members?

- All content is subject to normal school polices that apply to staff or pupils at the time of being submitted. As such, forum discussion will be treated as it was spoken within the school grounds.
- Users must own the rights to the content they submit and where necessary must refer to the original source fairly and legally. By agreeing to this policy you accept liability for any content you submit.

Visibility

- All users of the site must be aware that areas of the site may be publicly accessible to non-authenticated users outside of the school. Though the best effort will be made by the administrators to ensure that the privacy of users is kept.
- User account passwords must be kept private, though it is acceptable for parents/carers to use the same account. Students are expected to ensure that their parents/carers read and agree to the acceptable use agreement before being allowed to use that student's account. No other person apart from the staff, registered guests, students, parents/carers may login to the VLE.

- If a user is aware that their login user name and password has been compromised they must immediately contact a member of staff to have the account password changed.

Banning

- Failure to abide to this policy may result in a temporary or lifetime ban for the offending user.
- The user may have certain user privileges removed for a set or unlimited amount of time rather than a complete ban. The length and scope of the ban is subject to the offense and is to be decided by an administrator.
- The duration of the ban is subject to the nature and extent of the offense and to be the decision of an administrator.

Moderation of accounts

- Classteachers will act as moderators for their classes. Mrs McLeod will act as overall Administrator for those accounts.
- Moderators must actively ensure that the rules outlined in this policy document are abided by, within their jurisdiction, by all users, including each other and staff.
- Administrators will judge what is considered as misuse. Any misuse must be reported to an administrator.
- In the event of posted content breaching this agreement moderators must:

-Delete the content (i.e. a forum message) or edit it in order to censor the sensitive content.
-Warn the user (by posting a message or emailing them).
- If the incident is severe alert the e-safety co-ordinator or a senior member of staff immediately.
-A note of the offense under the user name should be noted.

Updates

- In the event that this policy document is updated users will be informed. In this event the user will be presented with the updated policy when logging on next and asked if they agree with the amended version.

Unauthorized access

- If a user finds that they do not have the correct user privileges they must report this to the moderator immediately.
- Any signs of unauthorized access onto the virtual learning environment must be reported to an administrator immediately. This includes a person using another person's user name and password to log in.

General Policy Decisions

Authorising Internet access

- All staff and Governors must read and sign the “Staff Code of Conduct for Computing” and the ‘Policy on Social Networking Websites’ before using any school Computing resource. This Policy will be reviewed each academic year.
- The school will maintain a current record of all staff and pupils who are granted access to school Computing systems.
- At Key Stage 1, access to the Internet will be by adult demonstration and with supervised access to specific, approved on-line materials.
- Parents/carers will be asked to sign and return a consent form.
- All staff and Governors will be asked to sign a School Computing Code of Conduct and the Policy on Social Networking Websites at the beginning of each academic year.
- Any person not directly employed by the school will be asked to sign an “acceptable use of school Computing resources” before being allowed to access the internet from the school site. E.g. Students / Work Experience.

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. The school can not accept liability for any material accessed, or any consequences of Internet access.
- The school should audit Computing use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

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 child protection procedures.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

Communications Policy

Introducing the e-safety policy to pupils

- e-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-Safety will be developed, possibly based on the materials from CEOP. (Child exploitation and online protection centre)

- e-Safety training will be embedded within the Computing scheme of work, the Personal Social and Health Education (PSHE) curriculum and will be of priority when accessing the internet for cross-curricular use .

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor Computing use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils and should pre-test any site that has not been used before.

Enlisting parents' and carers' support

- Parents/carers attention will be drawn to the School e-Safety Policy in newsletters and on the school Web site.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents/carers to sign the parent/carer/pupil agreement when they register their child with the school.

Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for Computing, bullying and for child protection. Due to the emerging technologies this policy is always under review.

- The school will appoint an e-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap. It is not a technical role.
- Our e-Safety Policy has been written by the school, building on government guidance. It has been agreed by senior management and approved by governors.
- The e-Safety Policy was revised by: Christopher Young
- It was approved by the Governors on:
- The next review date is (at least annually): January 2020

Christopher Young

(January 2019)

Appendix 1: Useful resources for teachers

Child Exploitation and Online Protection Centre
www.ceop.gov.uk

Childnet
www.childnet-int.org

Digizen
www.digizen.org

Kidsmart
www.kidsmart.org.uk

Think U Know
www.thinkuknow.co.uk

Appendix 2: Useful resources for parents/carers

Family Online Safe Institute
www.fosi.org

Internet Watch Foundation
www.iwf.org.uk

Internet Safety Zone
www.internetsafetyzone.com

Think U Know
www.thinkuknow.co.uk