E-Safety Policy

Ratified by the Governing Body in November 2016

Amended on 3rd November 2016

Updated on 1st September 2017

Review date: November 2018

Introduction

1.1. At West Blatchington Primary School, we recognise that the Internet can be used as an important tool for teaching and learning. We understand the need for children and staff to develop their skills, gain confidence and capability in using the Internet. We also respect the need for the Internet to be used appropriately at all times.

1.2. This policy applies to the governing body, all teaching and other staff, whether employed by Brighton & Hove City Council or employed directly by the school, individual governors, external contractors providing services on behalf of the school or the City Council, teacher trainees and other trainees, supply staff, agency workers, volunteers and other individuals who work for, or provide services on behalf of, the school. These individuals are collectively referred to as 'staff' in this policy.

2. Aims of the policy

2.1. The aims of the policy are:

- To provide guidelines for the appropriate use of the internet
- To ensure that a safe environment is created for all pupils in their use of the internet
- To monitor use of the Internet and exercise a duty of care to all pupils.
- To make sure that procedures are in place for the monitoring of security within school systems

3. Content

3.1. The school Internet accesses will be designed especially for pupil use and will include filtering appropriate to the age of pupils.

3.2. 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.

3.3. Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use.

4. Pupil Access

4.1. Pupils will use the Internet to access suitable educational sites that give information related to studies in the National curriculum. Websites will be introduced by teaching staff, and will have been viewed previously to determine suitability and appropriateness for the age group of the children.

4.2. Pupils (in Year 3) will not be given individual e-mail addresses, but will have the opportunity to e-mail under the direction of the class teacher using the school e-mail address.

4.3. Parents will be informed about the Internet policy at school.

5. Staff Access

5.1. Staff are able to access the Internet in connection with teaching and learning, using appropriate sites.

5.2. The Computer Misuse Act 1990 makes it an offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer".

5.3. It is important that staff ensure that no inappropriate material is viewed on school computers. Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.

5.4. Staff are allowed to use e-mail in connection with their professional duties and are allocated an individual e-mail address, via the alias system in operation.

5.5. Staff are allowed to use e-mail for personal use (outside school hours) but should be aware that mail sent via the BHCC proxy server is monitored for inappropriate content and attachments. Abuse of the Internet or e-mail by any BHCC employee is a serious matter that could result in disciplinary procedures.

5.6. All staff including administration, caretakers, governors, contracted service providers and helpers will be made aware of the E-Safety Policy and will need to sign to state that they have read and will adhere to the Policy. See Appendix 1.

6. Security of ICT systems

6.1. Checks on users files and history files will be reviewed regularly with regard to security and virus protection will be installed and updated regularly by IT technicians.

6.2. Unapproved system utilities and executable files will not be allowed in pupils work areas or attached to e-mail, and any files held on school's network will be regularly checked.

6.3. The school IT technicians will ensure that the system has the capacity to take increased traffic caused by Internet use.

6.4. All Internet content viewed in school is filtered using software to block offensive and inappropriate material. Childrens' use of the Virtual Learning Environment (Bumble) is regularly monitored.

6.5. Emails and messages are carefully monitored and as are swear words/bullying/or other inappropriate language. There is a whistle icon on the top left hand side of the screen. If a child or parent feels there is inappropriate material/emails being sent you can click on the whistle icon. This notifies both the ICT coordinators and the service provided and we will ensure action is taken and the matter is investigated. See T:\Subject leader folders\ICT co-ordinator\VLE\VLE2013-2104\ letter to parents for further details.

7. Password security

7.1. To secure the data held within the School and prevent unauthorised access to systems and applications, it is imperative that all staff members create strong passwords for all of the ICT applications and equipment that they use within the School.

7.2. It is recommended that passwords contain at least 8 characters and include at least one upper case letter, one lower case letter and one number.

7.3. Passwords should not include personal details such as date of birth, name, friends and family names or telephone numbers.

7.4. Every effort should be made to remember passwords without the need for writing them down. If a password must be written down, staff members are to ensure that the written document is securely stored away to prevent it being viewed by others.

8. Viewing of confidential or sensitive information

8.1. Staff members should always be aware of who can view the information they see whilst working on a computer or electronic device. Particular attention should be taken when

working in a classroom or public area and to ensure that their screen is not reflected onto a surface or visible from a window.

8.2. When leaving a computer or electronic device unattended, staff members must always ensure that they either log off or lock the device (e.g. ctrl+alt+del on a computer) to prevent unauthorised use. This is especially important when using computers in the classroom.

8.3. After school trips and off site events, all pupil information (including parent contact information) that has been printed must be shredded after the trip.

9. Encrypted Email

9.1. The Data Protection Act requires you to take measures to prevent unauthorised access or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.

9.2. All personal and sensitive information needs to sent using the Egress encrypted email system if it is sent to anyone outside the school 365 email environment.

9.3. Personal information is:

- Defined as any combination of data items that identifies an individual and provides specific information about them, their achievements and their families
- That could include: names, contact details, gender, dates of birth, unique pupil number etc.
- It could also include: academic achievements, skills and abilities, progress, behaviour and attendance

9.4. Sensitive data is specifically defined as information relating to:

- a person's racial or ethnic origin
- political opinions
- religion or beliefs
- membership of a trade union
- physical or mental health
- sexual life
- alleged offence or any proceedings for any offence

10. School website

10.1. We shall ensure that any information on West Blatchington Primary School's website reflects the school ethos, is accurate and well presented, and that personal security is not compromised.

10.2. The point of contact on the website will be the school address, school e-mail and telephone number. Staff or pupil's home information will not be published.

10.3. Website photographs will be carefully selected and will not enable individual pupils to be identified. Written permission from parents or carers will be obtained before any photographs are used.

10.4. The Head Teacher or nominee will take overall editorial responsibility and ensure that information is accurate and appropriate.

10.5. The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

10.6. Comments and text on the website will comply with the guidelines in the School's Social Networking Policy.

11. Virtual Learning Environment

11.1. Purple Mash was introduced in the Summer 2017 term and will be rolled out fully in Autumn 2017, providing children with increased online learning opportunities.

11.2. Further updates to this policy section will follow in Autumn 2017.

12. iPads

12.1. iPads are a valuable tool within electronic learning and are used across year groups within Key Stage 1 and Key Stage 2.

12.2. All iPad accounts are to be set up under the School iTunes account to ensure appropriate access to educational platforms and prevent inappropriate information, images and apps being viewed within the School.

12.3. Staff members must not under any circumstances, set up a personal iTunes account on a School iPad. This is to prevent staff members' personal information and images being inadvertently displayed on an iPad within the School.

12.4. All School iPads must be stored securely on the lockable trolleys provided.

13. Mobile Phones

13.1. Many mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

13.2. Pupils by permission of the Head teacher can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are to be turned off and handed into the school office at 8:45, then collected at the end of the day.

13.3. The sending of abusive or inappropriate text messages is forbidden.

13.4. Staff should always use the school phone to contact parents.

13.5. Staff, as well as students and visitors, are not permitted to access or use their mobile phones within the classroom. Staff must ensure that their phones are turned off and stored safely away during the teaching day.

13.6. Staff may use their mobile phones in the staffroom during the lunch period.

13.7. Staff must not use the school wifi for personal mobile devices or smart watches.

13.8. Parents cannot use mobile phones on school trips to take pictures of the children.

14. USB Sticks

14.1. In order to preserve data security, only encrypted USB sticks should be used to temporarily transfer school data, particularly information of a confidential or sensitive nature.

14.2. Unencrypted USBs sticks can only be used for temporarily transporting data that is low level (green) rated.

14.3. USBs (whether encrypted or not) must never be used to permanently store data, as a backup facility or to transfer and upload school information to a staff member's personal computer device.

15. Personal computers

15.1. Dependent on the requirements of their role, selected staff will be allocated a school laptop or remote access link e.g. via log me in, to enable them to work securely at home.

15.2. Personal computers must not be used to store School information. If it was found that a computer had been used for storage of school records (even if temporarily), when it was due for disposal, it would need to be forensically wiped to CESG Infosec Level 5 HMG standards by the School's IT providers to ensure no future access to sensitive data.

15.3. It is important that all staff members are aware that if school data is breached from their personal computer it is their responsibility.

16. Expectations

16.1. Internet access will be available to all pupils and staff. It is an expectation that all staff and pupils comply with the statements set out in this policy.

17. Implementation

17.1. Implementation of the policy is the responsibility of all staff.

18. Review

18.1. This policy will reviewed, together with the ICT Acceptable Use Policy and Social Networking Policy every two years.

Appendix 1 – Copy of the Staff ICT Policies Agreement Form

Staff ICT Policies Agreement

Covering ICT Acceptable Usage Policy, E-Safety Policy and Social Networking Policy

E-Safety Policy & Social Networking Policy

Summary of Key Guidelines:

- The school owns the computer network and can set rules for its use.
- It is an offence to use a computer or network for a purpose not permitted by the school.
- Network access **must** be made via the user's authorised account and password, which must not be given to any other person (i.e. colleagues or supply teachers)
- You **must** remember to log off your computer and email account to ensure child protection whenever you are not at your PC.
- All network and internet use **must** be appropriate to education within school working hours.
- Copyright **must** be respected (images used must be copyright free).
- Messages shall be written carefully and politely particularly as emails could be forwarded to unintended readers.
- Anonymous messages and chain letters are **not** permitted.
- Do **not** browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Use of websites for personal financial gain, gambling, political activity, advertising or illegal purposes is **not** permitted (however, viewing a trade union site is permitted).
- Staff must not use the school wifi for their own mobile devices including smart watches.
- **Do not** give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents or carers. Always provide outside agencies with the school contact details and your school email address.
- The use of mobile phones is **not** permitted in the presence of children. Photographs and videos of children **must not** be taken on mobile phones (see Safeguarding Policy).
- School mobile phones should be used during residential trips and day visits. Personal mobile phones should **not** be used to contact parents. There is a school mobile phone on each site.
- Personal cameras (including those on mobile devices) **must not** be used in school or during out of school hours events. Always use school cameras for photographing children and **do not** store photographs on your school laptop or memory sticks.
- After school trips and off site events, all pupil information (including parent contact information) must be shredded after the trip.
- Ensure that your online activity, **both in school and outside school**, will not bring your organisation or professional role into disrepute.
- Do **not** state that you work at West Blatchington Primary & Nursery School on any personal social media site or online profile, to ensure that any personal opinions do not reflect upon or link to the school.

You have a duty to report any E-Safety incident which may impact on you, your professionalism or your organisation.

The use of social networking sites is permitted **but** staff are reminded to use them in a **professional manner** and according to the guidance set out in the ICT Acceptable Usage Policy, E-Safety Policy and Social Networking Policy.

I hereby agree to the above rules. I also confirm that I have read and will adhere to both the E-Safety & Social Networking Policies and that it is my responsibility to keep up to date with the school's most recent policies.

Signed: _____ **Date**: _____

ICT Acceptable Use & Information Security Policy

I have read and understood West Blatchington Primary & Nursery School's ICT Acceptable Use & Information Security Policy and agree to abide by all the points above in this document and its guidelines and recommendations during my time of employment at West Blatchington Primary & Nursery School.

I understand that all school information that I have access to during my employment remains the property of the school following the termination of my employment at the school. I agree not to divulge any information inappropriately according to this policy following the termination of my employment at the school.

I understand that it is my responsibility to ensure that I remain up to date and read and understand the school's most recent policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signed: _____ **Date**: _____

Print Full Name: _____

Job Role: _____