Bracken Hill School

Responsible Internet Use Policy / E-Safety Policy

Author: Mrs Clerkin

Policy Type: Whole School

This policy is reviewed bi-annually to ensure compliance with current regulations

The Governors of the school recognise that all staff play a vital role in the achievement of high standards and in providing our pupils with the best opportunities matched to their needs.

Three of our published Educational Aims are:

- We aim to help each pupil develop the skills they need towards independent and responsible living.
- We aim to provide pupils with a wide range of age appropriate experiences that helps to foster functional daily life resilience.
- We aim to help develop relationships characterised by kindness, helpfulness and respect.

Policy development

The e-safety policy is part of the School Improvement Plan and relates to other policies including those for ICT, Social Media Policy,
Anti-bullying and Safeguarding Children.

- Our policy has been written with full consultation from staff in school, parents/carers, governors and young people.
- It has been agreed by senior leaders and approved by governors.
- The policy and its implementation will be reviewed annually.
- It is available to read or download on our school website or as a hard copy from the school office.

Roles and responsibilities

Our co-ordinator is Kath Harris

Teaching and Learning

Why internet and digital communications are important

- The purpose of any technology in school is to raise educational standards, to promote achievement, to support the professional work of staff and to enhance the school's management functions.
- The school has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for staff.
- Pupils will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- They will be encouraged to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be shown how to publish and present information appropriately to a wider audience.
- They will be taught what internet use is acceptable and what is not and be given clear objectives for use. These are also important transferable skills for their life out of school, including using mobile phones and other mobile devices.
- They will be taught how to report unpleasant internet content including Cyberbullying or unwanted contact.
- Issues such as Cyberbullying and e-safety will be built into the curriculum to encourage self –efficacy and resilience. Some children who have had problems or with additional needs may need additional support.

Managing Internet Access

Information security system

- The school ICT system security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies may be discussed with the Local Authority

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a member of staff if they receive offensive e-mail.
- Staff to pupil e-mail communication must only take place via a school e-mail address or from within a learning platform and will be monitored.
- All incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school website

- The contact details on the school's website should be the school address. No staff or pupil's personal details will be published
- The Head Teacher or their nominee will have overall editorial responsibility to ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include children will be selected carefully and will not enable individuals to be clearly identified unless permission has been granted.
- Pupil's full names will be avoided on the website and learning platforms including blogs, forums especially if associated with a photograph.
- Written permission will be obtained from parents and carers before any photographs are published on the school website.
- Parents should be clearly informed of the school policy on image taking and publishing.

Social networking and personal publishing on the school learning platform

- The school will control access to social networking sites and consider how to educate pupils in their safe use. This may not mean blocking every site; it may need monitoring and educating students in their use.
- The school will encourage parents to support their children when setting up a social networking profile and offer help and guidance. This includes encouraging families to follow the terms and conditions specifying the appropriate age for using sites.
- Pupils will be advised never to give out personal details which may identify them or their location.
- Cyber bullying and its consequences will shared with the children and strategies for keeping them safe will be taught regularly.

Managing filtering

- The school will work with the County Council to ensure systems to protect pupils are reviewed and improved.

- Any unsuitable on-line material should be reported to the e-safety coordinator and logged on the e-safety log sheet.
- Regular checks will be made to ensure the filtering methods are appropriate, effective and reasonable.
- A log will be kept and used to identify patterns and behaviours and therefore inform policy and educational interventions.

Managing video conferencing

- Video conferencing will be appropriately supervised for the pupils' age.
- Pupils will always ask permission from the supervising teacher before making or receiving a video conference call.
- Video conferencing will use the educational broadband network to ensure quality of service and security.

Managing emerging technologies

- The school will examine emerging technologies for their educational benefit and carry out a risk assessment before use in school.
- Mobile phones and associated cameras will not be used in lessons or formal school time except as part of an educational activity.
- Care will be taken with the use of hand held technologies in school which may not have the level of filtering required.
- Staff will use a school phone where contact with pupils and their families are required.

Protecting personal data

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

Policy decisions

Authorising internet access

- All staff must read and sign the 'staff code of conduct' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are given access to school IT systems.
- Parents will be asked to sign and return a consent form.
- Access to the internet will be by adult demonstration with directly supervised access to specific on-line materials.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the internet from the school site.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material; however it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school will monitor ICT use to establish if 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.
- Complaints of misuse by staff will be referred to the Head Teacher.
- Any complaints of a child protection nature must be dealt with in accordance to child protection procedures.
- Pupils and parents will be informed of the consequences and sanctions for pupils misusing the internet and this will be in line with the schools behaviour policy.

Community use of the internet

- All use of the school internet connection by community and other organisations shall be in accordance with the e-safety policy.

Communicating the policy

Policy dated: June 2019 – Approved by the Governing Body on 2 July 2019

Pupils

- Appropriate elements of the e-safety policy will be shared with pupils.
- Pupils will be informed that network and internet use will be monitored.
- Age appropriate curriculum opportunities will be used to ensure all pupils gain an awareness of e-safety. These will be addressed on a regular basis and modified as newer risks are identified.

Staff

- All staff will be given a copy of the e-safety policy and required to sign to acknowledge that they have read and understood the policy and agree to work within the guidelines.
- Staff should be aware that the system is monitored and that professional standards are expected.
- Staff monitoring the system will be supervised by senior management and have a clear procedure for reporting.

Parents

- Parents will be notified of the policy in newsletters, the school brochure and website.
- All parents will be asked to sign the parent/pupil agreement when they register their children.
- Parents will be offered e-safety training to encourage them to support and encourage positive online activities with their children and help them to use the internet safely.

This Policy will be reviewed annually

Appendix 1

Bracken Hill School

Smile and stay safe.

- **S**taying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location).

- **M**eeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

- **I**nformation online can be untrue, biased or just inaccurate. Someone online may not be telling the truth about who they are – they may not be a 'friend'.

- **L**et a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

- **E**mails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Appendix 2
(Taken from WHOLE SCHOOL SAFEGUARDING AND CHILD PROTECTION POLICY 2016).

Child Sexual Exploitation (CSE) Policy

Policy dated: June 2019 – Approved by the Governing Body on 2 July 2019

The school adheres to the NSCB procedure in relation to child sexual exploitation. This is our policy to summarise our position.

We recognise that child sexual exploitation is a high profile issue both nationally and locally.

The school recognises that the child sexual exploitation can cause a great deal of harm to a child, including physically, emotionally, educationally and socially. Where it exists it can also cause harm to communities including our school.

Child sexual exploitation can happen in a number of ways to both boys and girls, for example it can happen in the virtual world through various social media and this can still cause significant harm. It can happen though inappropriate relationships such as older boy/girlfriends or through parties, gangs or organised abuse. Some children will be particularly vulnerable to being exploited, for example if they have had a chaotic upbringing or if they are in care or go missing, involved in gangs or being bullied. We recognise however that any child can become a target for exploitation, particularly where the internet and social media are involved. This is because the normal life events that go with being a child or teenager in today's age can be a challenge and make them susceptible to being groomed and exploited.

As a school we recognise that prevention is the best position with regard to CSE. We seek to support children to develop confidence and build resilience. We will endeavour to support their age appropriate knowledge and raise awareness and understanding of what CSE is, to understand the risks of CSE and to spot the warning signs for themselves and also their friends and peers and by doing so keep safe.

If prevention is not possible we aim to identify children who are at risk of, or being exploited very early. Early intervention is key to effectively working with the child to prevent or reduce the level of risk. Once they have been groomed some children will find it difficult to withdraw from their abusers and we need to contribute to helping to protect them. Some children feel that they are in a relationship with these people. We commit to working with our inter-agency partners to safeguard and protect children.

Much of this work will be through our programmes of personal, social and health education (PSHE) .

An important part of educating our children is focussing on what is a healthy relationship and issues of consent. This will also target potential abusers at an early age with the intention of helping to shape their attitudes to others.

We want to have a culture where the welfare of children is actively promoted and staff and pupils are vigilant. As part of this children will feel listened to and safe.

Policy distributed to Governors September 22nd 2015
Policy to be ratified at next Pupil and Personnel meeting in October 2015

Appendix 3

(Taken from WHOLE SCHOOL CYBER BULLYING POLICY 2019)

Cyber Bullying Policy

Policy dated: June 2019 – Approved by the Governing Body on 2 July 2019

Bracken Hill educates its pupils both in the proper use of telecommunications and about the serious consequences of cyber-bullying and will, through PSHE and in ICT lessons and assemblies, continue to inform and educate its pupils in these fast changing areas.

Bracken Hill trains its staff to respond effectively to reports of cyber-bullying or harassment and has systems in place to respond to it. Bracken Hill endeavours to block access to inappropriate web sites, using firewalls, antivirus protection and filtering systems and no pupil is allowed to work on the internet in the Computer Room, or any other location within the school which may from time to time be used for such work, without a member of staff present. Where appropriate and responsible, Bracken Hill audits ICT communications and regularly reviews the security arrangements in place.

Whilst education and guidance remain at the heart of what we do, Bracken Hill reserves the right to take action against those who take part in cyber-bullying.

- All bullying is damaging but cyber-bullying and harassment can be invasive of privacy at all times. These acts may also be criminal acts.
- Bracken Hill supports victims and, when necessary, will work with the Police to detect those involved in criminal acts.
- Bracken Hill will use, as appropriate, the full range of sanctions to correct, punish or remove pupils who bully fellow pupils or harass staff in this way, either in or out of school.
- Bracken Hill will use its power of confiscation where necessary to prevent pupils from committing crimes or misusing equipment.
- All members of the School community are aware they have a duty to bring to the attention of the Head any example of cyber-bullying or harassment that they know about or suspect.

Appendix 4 (Taken from WHOLE SCHOOL SOCIAL MEDIA POLICY)

Use of Social Media in the classroom

- Supervision in the classroom with social media technology must be appropriate to the children's needs and abilities;
- It is good practice for staff to evaluate websites before classroom use. Staff should be aware that websites, search results etc. may be safe and appropriate one day but unsafe a day later. All members of the school

community should be aware that filtering software is not always effective and cannot always be relied on alone to safeguard children;

- Children with Special Educational Needs should be appropriately supported according to their specific needs and their personal understanding of the e-Safety risks;
- All pupils and staff should be aware of the school procedure regarding what to do if inappropriate content or messages are found, sent or received online;
- All pupils and staff should understand how to critically evaluate online content;
- Internet filtering must be in place according to the school's requirements. This should be designed with both a technical and curriculum focus and should be agreed by the schools Leadership Team and Governors;
- ICT tools provided by the school should always be used (e.g. work provided digital cameras, memory cards, laptops etc.) rather than personally owned equipment.