Blatchington Mill School

Online Safeguarding Policy

Date Policy Created:	February 2020
Date of last amendment:	December 2018
Date to be reviewed:	February 2022

Contents

1. Policy creation

Our online safeguarding Policy has been written by the school, building on the government's policy on Keeping Children Safe in Education, UK Council for Internet Safety, Brighton and Hove model e-safety Policy, NSPCC, CEOP, national education network and other government guidance. It has been agreed by the Senior Leadership Team and approved by Governors. The Online Safeguarding Policy and its implementation will be reviewed every two years.

Initiated:	April 2010 Groups
Consulted:	Governors Staff
Date Reviewed:	February 2020
Review date:	February 2022
Audience	Parents/Carers Staff Governors Students y
Policy located:	School Website (Staff and Parents/Carers)
Policy Format:	Full
Lead Member of Staff:	Roomee Ahmad (Head of Computer Science)

2. Teaching and learning

2.1 The importance of Internet use

- The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Students use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security

2.2 Benefits of the Internet to education

Benefits of using the Internet in education include:

- access to world-wide educational resources
- inclusion in the National Education Network which connects all UK schools
- educational and cultural exchanges among students and organisations worldwide
- access to experts in many fields for students and staff
- professional development for staff through access to national developments, educational materials and effective curriculum practice
- collaboration across support services and professional associations
- improved access to technical support including remote management of networks and automatic system updates
- exchange of curriculum and administration data with Examination Boards and other organisations
- access to email facilities
- access to learning wherever and whenever convenient.

2.3 Using the internet to enhance learning

- The school Internet access will include filtering appropriate to the age range of students and monitoring of its use to provide audit trails.
- Students will be taught what Internet use is acceptable and what is not and given clear guidance for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff will guide students in online activities that will support the learning outcomes planned for the students' age and maturity.

- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.4 Evaluation of Internet content

- The school will reinforce the concern that copying and subsequent use of Internet derived materials by staff and students must comply with copyright law.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of online materials is a part of every subject area's teaching.
- Students will be taught to change the privacy settings on their online profiles
- Students will be taught about reporting inappropriate contents to a member of staff or to the network team
- All members of staff to inform the network office about any inappropriate content

3. Managing Information Systems

3.1 Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Unapproved system utilities and executable files will not be allowed in students' work areas or attached to email.
- Student files are stored on Google's cloud storage which provides one of the most secure storage of data in the world.
- Staff files are stored on Google's cloud storage and some files are still stored on local network drives. The local drives are backed up regularly.
- All users of the system will agree to the school's Acceptable Use Policy.

3.2 Email

- Students may only use approved email accounts.
- Staff will use only their official school email account when communicating with students via email.
- If a student receives offensive email they should report it immediately.
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and may be restricted.
- Email sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

3.3 Management of published content

- The contact details on public facing websites should be the school address, email and telephone number. Staff or students' personal information must not be published.
- The Headteacher will take overall editorial responsibility for accuracy of published content.
- The school websites should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

3.4 Publishing of Student images

- Students will be taught the reasons for caution in publishing personal information and images in social publishing sites (see section 3.5).
- Generally photographs for school and family use and those that appear in the press are a source of pleasure and pride. They usually enhance self esteem for children and young people and their families and the practice should continue within the following safe practice guidelines.
- Parents and carers will be given the opportunity annually to prohibit their child's photograph from appearing in any externally published content, and specifically websites.
- Images that include students will be selected carefully and will not enable individual students to be identified by name without permission of their parents or carers.
- When using images of children, such images will portray children in suitable dress. Care will be taken, photographing PE or swimming events to maintain modesty, using tracksuits if appropriate for example.
- It is the responsibility of the teacher requesting publication to check (e.g. on SIMS) that the school has permission to publish images of every identifiable student featuring in any particular photograph they submit for publication.
- Consent of parents or carers must be obtained before any child can appear in a video. Parents or carers can make their own video recordings of productions and other such events for their own personal and family use, as they are not covered by the Data Protection Act.
- Work can only be published with the permission of the student.
- Staff should not store images of students in personal areas e.g. on memory sticks, or on home PCs. While in school, student images must be stored securely.

3.5 Management of social networking and personal publishing

Examples include: Facebook, Snapchat, Instagram, WhatsApp, Twitter, YouTube, TikTok, Windows Live Spaces, Oovoo, KIK, Flickr, Tumblr, forums, bulletin boards, multiplayer online gaming, chatrooms, Instant Messenger and many others.

Staff members should also read the school's Social Networking Policy for BHCC Schools and BMS Social media policy.

- The school will block/filter access to social networking sites other than those approved by the school for use in school.
- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends, specific interests and clubs etc.
- Students will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice will be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
- Students will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students will be encouraged to invite known friends only and deny access to all others.
- Students will be advised that allowing access to a friend on their social network space could allow access by friends of that friend, who would be unknown to the student.
- Students will be advised not to publish specific and detailed private thoughts.
- Staff official blogs or wikis will be password protected and run within the school. Teachers will be strongly advised not to run social network spaces for student use on a personal basis.
- Staff should not befriend, seek to befriend, or communicate with students on any social networking site outside the official school system.
- Staff will be advised not to quote Blatchington Mill, or any of the student / staff population therein, by name on any personal / social networking site.
- Staff and students should not contribute any material online which may bring the school into disrepute.
- Staff and students will be aware that bullying can take place through social networking especially when a space has been set up without a password and others are invited to make/see comments.

3.6 Web Filtering

- The school's Network Services team works with internet content filters at Brighton and Hove Council, our own filters onsite, a Threat Management Gateway firewall, the Securus network activity monitoring system and with organisations such as CEOP to ensure that systems are in place to protect students.
- If staff or students discover unsuitable sites, the URL must be reported to Network Services, and not passed to other students for their use.
- As well as the Education Authority filtering, the school also manages its own filtering systems.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any behaviour that the school believes is illegal must be reported to appropriate agencies such as CEOP.

3.7 Video conferencing

Network Services can allocate Google Hangouts / Meet to staff laptops for this purpose. Staff should contact network services to enable camera and microphone access for the video conferencing.

- The use of Google Hangouts / Meet within school at this time is to be used to contact external agencies such as schools only.
- Staff should sign up to Google Hangouts / Meet using their school email address
- The username and password should be kept secure and not be saved on the laptop
- For their own protection Google Hangouts / Meet should be used by staff strictly for school business only, and should not be used to contact students directly.
- When our students are to be included in a video conference it is the responsibility of the member of Blatchington Mill staff leading the video conference to ensure that the content of the conference is suitable for the students.
- Videoconferencing should be supervised appropriately for the students' age.
- When recording a video conference lesson, permission should be given by all participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.
- Recorded material must be stored securely.

3.8 Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Only reliable and GDPR compliant cloud-based systems can be used if students and/or staff are required to register to use the service.
- Mobile phones will not be used during lessons or formal school time unless with the express permission of a teacher for a recognised educational benefit to that lesson.
- The sending of abusive or inappropriate E- messages of any sort is forbidden. E.g. Snapchat, KIK/ Whatsapp text messages, Instagram video or multimedia image messages.
- Teaching staff may make use of infrared or Bluetooth communication technologies in the classroom if they wish to and if they are satisfied that data security will not be breached.
- Staff will be issued with a school phone where contact with students is required. Private mobile phone numbers will not be given to students by staff.
- Staff who wish to use their own personal digital devices on the school wireless network will be required to register their device with Network Services in order to gain access to the network.
- Permanent wireless access points are located throughout the school site in line with the schools Technologies Development Plan. The school will endeavour to provide temporary wireless access to the network in any area of the school where it is required, provided adequate notice is given to Network Services.

3.9 Protection of personal data

- Personal data will be recorded, processed, transferred and made available according to the general data protection regulations(GDPR).

4. Policy Decision

4.1 Authorisation to use the internet

- The school will maintain a current record of all staff and students who are granted access to the school's electronic communications.
- All staff must read and sign the Acceptable Use Policy before using any school ICT resources.
- Parents/ carers will be informed that students will be provided with filtered Internet access.

4.2 Risk Assessment

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Students will be made aware of how to avoid unsuitable content, and the steps to take if they are faced with it. However, the school cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- The school audits ICT use to establish that the Online Safeguarding policy is adequate and that the implementation of the Online Safeguarding policy is appropriate.
- 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 school recognises that withdrawal of computer and Internet facilities for a student could have a detrimental effect on that student's progress and coursework grades. However the school will withdraw access in cases where it is deemed necessary.

4.3 Online Safeguarding complaints procedure

- 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.
- Students and parents or carers will be informed of the complaints procedure.
- Parents/carers and students will need to work in partnership with staff to resolve issues.
- Discussions will be held with the Police School Liaison Officer to establish procedures for handling potentially illegal issues.
- Sanctions within the school behaviour policy include:
  - interview/counselling by the Heads of Year and/or Assistant Year team leaders ;
  - informing parents or carers;
  - removal of Internet or computer access for a fixed period.
  - removal of Internet or computer access permanently.
  - involvement of outside agencies including the police

4.4 Community use

- The school will liaise with external organisations to establish a common approach to Online Safeguarding.
- The school will be sensitive to Internet related issues experienced by students out of school, e.g. social networking sites, and offer appropriate advice.

5. Communications Policy

5.1 Policy implementation

- Online Safeguarding awareness and information will be displayed in school.
- Students are informed that all network and Internet use is monitored.
- An Online Safeguarding training programme is in place to raise the awareness and importance of safe and responsible Internet use.
- Online Safeguarding training and advice is included in the PSHE and Computing programmes covering both school and home use. Health commissioners, assemblies, parents and carers training are included during the year and materials available via school communications.
- Add CEOP button for reporting into the school's internal homepage

5.2 Staff sharing of Online Safeguarding policy

- All staff will be given the School Online Safeguarding Policy and its application and importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school Online Safeguarding Policy will be provided as required.

5.3 Parental/ Carer involvement

- Parents and carers' attention will be drawn to the school's Online Safeguarding Policy on the school brochure and on the school website.
- Internet issues will be handled sensitively, and parents/carers will be advised accordingly.
- A partnership approach with parents/ carers is encouraged. This includes parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents/carers.
- Our website includes a safeguarding → online section under the parents section which provides inks to targeted advice, guidance and materials for parents/carers, as well as the school Online Safeguarding policy.
- Interested parents and carers are referred to the organisations listed in section 6 'Online Safeguarding Contacts and References'.

6. Legislation

6.1 General Data Protection Regulations (GDPR)

Computer systems store lots of personal details, and personal data can be very valuable. This data needs to be protected and only used for the intended purpose. . The **GDPR** sets out principles that govern:

- who can access data
- the accuracy and validity of data
- selling data

6.2 The Computer Misuse Act

The Computer Misuse Act makes it an offence to:

- access computer material without permission, eg looking at someone else's files
- access computer material without permission and with intent to commit criminal offences, eg hacking into your bank's computer and increasing the money in your own account
- alter computer data without permission, eg writing a virus to destroy someone else's data

6.3 Sexual Offences Act 2003

Includes the offence of sexual grooming. But action can only be taken by authorities where it can be proved an adult intended to meet a child. Increasingly, online abusers have no intention of meeting the child physically. They may, for example, persuade a child to perform sexual acts via a webcam.

6.4 Malicious Communications Act 1988

Makes it an offence to send a communication with the intention of causing distress or anxiety. But the intent to cause distress or anxiety can be difficult to prove because online groomers do the opposite to this. They may find out a child's interests from their online profile and use these to send messages aiming to build a rapport with the child they've targeted.

6.5 Communications Act 2003 Section 127

Section 127 makes it an offence to send an electronic message that is grossly offensive or of an indecent, obscene or menacing character. An online groomer may not be covered by this law because they may send messages that aim to build up trust with a child.

7. SEND

7.1 Education and training

When teaching about online safety, learners with SEND may need:

- Complex online safety issues to be broken down and explained in greater detail
- To explore issues in a variety of contexts and approaches
- More examples of safe and unsafe practices
- Constant reinforcement and repetition of key safety messages
- Differentiated teaching resources and materials

7.2 Acceptable use rules

Some learners with SEND may intentionally test boundaries and contravene the rules; consider presenting consequences alongside the rules (i.e. cause and effect).

Acceptable use policies should also be shared with parents and carers to ensure that rules and consequences are consistent, both at school and at home.

- A learner who has difficulty transferring rules, or applying them out of context, may find constant reinforcement and visual reminders near the computer helpful.
- A learner who is allowed unrestricted access to technology at home and intentionally tries to bypass school filters may require a strict AUP which is shared and supported by parents/carers.

7.3 Engaging parents and carers:

Parents and carers play a vital role in supporting their children learn how to be safe online, but they can sometimes be particularly difficult to engage with; concerns about insufficient computer skills or a limited understanding about the online environment can be off-putting for many parents/carers, regardless of whether their child has SEND or not.

- Reassure parents/carers that online safety has more to do with parenting than technology
- Their child is likely to be vulnerable both on and off-line, so encourage parents/ carers to adopt similar mechanisms for supporting their child online, as they use in the real world.

7.4 Reporting concerns:

Learners with SEND may require a range of methods to enable them to report concerns and seek support. For example

- A learner, who is non-verbal, may require a messaging or sound system on their devices to help them to get adult attention.
- Learners may have 1-2-1 workers or trusted adults that they prefer to speak to who will be able to support the DSL in communicating with the learner.

8. Online Safeguarding Contacts and References

Childline

http://www.childline.org.uk/

Child Exploitation & Online Protection Centre

http://www.ceop.gov.uk

Childnet International

http://www.childnet.com

Internet Matters.org

http://www.internetmatters.org/

Internet Watch Foundation

http://www.iwf.org.uk/

UK Safer Internet Centre

https://www.saferinternet.org.uk/

NSPCC

https://www.nspcc.org.uk/keeping-children-safe/online-safety

Think U Know website

http://www.thinkuknow.co.uk/

Vodafone Digital Parenting

https://parentzone.org.uk/parents