Online safety

Contents:

Statement of intent

At Broadbottom CE(VC) Primary we encourage the safe use of online platforms as a valuable aspect of teaching and learning, raising educational standards and promoting pupil achievement

The use of online platforms is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into three areas of risk:

- Content: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.

- Contact: Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.

- Conduct: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

The measures implemented to protect pupils and staff revolve around these areas of risk. This policy has been created with the aim of assuring the appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

1. Legal framework

1.1 This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- DfE (2020) 'Keeping children safe in education'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- UK Council for Child Internet Safety (2017) 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'

1.2. This policy operates in conjunction with the following school policies:

- Cyberbullying Policy
- Social Media Policy (Currently under review)
- Acceptable Use Agreement
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy (Currently under review)
- PSHE Policy
- RSE and Health Education Policy
- Staff Code of Conduct
- Behavioural Policy
- Data Protection Policy
- SJF Online Learning Plan

2. Roles and responsibilities

2.1. The governing board is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the Computing Co-ordinator remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training (including online safety) at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.

2.2. The headteacher is responsible for:

- Supporting the Computing Co-ordinator and any deputies by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the subject co-ordinator and ICT technicians to conduct regular light-touch reviews of this policy.
- Working with the subject co-ordinator and governing board to update this policy on an annual basis.

2.3. The subject leader is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.

- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.

- Liaising with relevant members of staff on online safety matters, e.g. the SENDCO and ICT technicians.

- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.

- Ensuring safeguarding is considered in the school's approach to remote learning.

- Ensuring appropriate referrals are made to external agencies, as required.

- Staying up-to-date with current research, legislation and online trends.

- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.

- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.

- Ensuring all members of the school community understand the reporting procedure.

- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.

- Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's procedures.

- Reporting to the governing board about online safety on an annual basis.

- Working with the SLT and ICT technicians to conduct termly light-touch reviews of this policy.

- Working with the SLT and governing board to update this policy on an annual basis.

2.4. ICT technicians are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.

- Implementing appropriate security measures as directed by the SLT.

- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

- Working with the subject co-ordinator and SLT to conduct termly lighttouch reviews of this policy. 2.5. All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.

- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Reporting concerns in line with the school’s reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

2.5. All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Reporting concerns in line with the school’s reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

2.6. Pupils are responsible for:

- Adhering to this policy, the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer has experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

3. The curriculum

3.1. Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- PSHE
- Computing

3.2. The curriculum and the school’s approach to online safety is developed in line with the UK Council for Child Internet Safety’s ‘Education for a Connected World’ framework and the DfE’s ‘Teaching online safety in school’ guidance.

3.3. Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

3.4. Online safety teaching is always appropriate to pupils' ages and developmental stages.

3.5. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- Use of Passwords & why they are important
- Showing respect online
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Understand Digital Footprints

3.6. The online risks pupils may face are always considered when developing the curriculum.

3.7. The subject leader is involved with the development of the school's online safety curriculum.

3.8. The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

3.9. Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils

3.10. External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The SLT and subject co-ordinator decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

3.11. Before conducting a lesson or activity on online safety, the class teacher and subject co-ordinator consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The subject co-ordinator advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity.

3.12. Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

3.13. During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and are not worried about getting into trouble or being judged.

3.14. If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with sections 15 and 16 of this policy.

3.15. If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in sections 15 and 16 of this policy.

4. Staff training

4.1. All staff receive safeguarding and child protection training, which includes online safety training, during their induction.

4.2. Online safety training for staff is updated annually.

4.3. In addition to this training, staff also receive regular online safety updates as required and at least annually.

4.4. The subject co-ordinator undergoes training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training.

4.5. In addition to this formal training, the subject co-ordinator and any deputies receive regular online safety updates to allow them to keep up with any developments relevant to their role. In relation to online safety, these updates allow the subject co-ordinator to:

- Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and capability required to keep pupils safe while they are online at school.
- Recognise the additional risks that pupils with SEND face online and offer them support to stay safe online.

4.6. All staff receive a copy of this policy upon their induction and are informed of any changes to the policy.

4.7. Staff are required to adhere to the Staff Code of Conduct at all times, which includes provisions for the acceptable use of technologies and the use of social media.

4.8. All staff are informed about how to report online safety concerns, in line with sections 15 and 16 of this policy.

4.9. The subject co-ordinator acts as the first point of contact for staff requiring advice about online safety.

5. Educating parents

5.1. The school works in partnership with parents to ensure pupils stay safe online at school and at home.

5.2. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parental awareness is raised in the following ways: • Newsletters

- Weblinks on school website and school social media sites.
- Publication material

5.3. Parents are sent a copy of the Acceptable Use Agreement and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

6. Classroom use

6.1. A range of technology is used during lessons, including the following:

- PCs
- Laptops
- Tablets

6.2. Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource.

6.3. Class teachers ensure that any internet-derived materials are used in line with copyright law.

6.4. Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

7. Internet access

7.1. Pupils, staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement.

7.2. All members of the school community are encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

8. Filtering and monitoring online activity

8.1. The SLT and governing board ensures the school's ICT network has appropriate filters and monitoring systems in place.

8.2. The subject co-ordinator and ICT technician undertake a risk assessment to determine what filtering and monitoring systems are required.

8.3. The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.

8.4. The subject co-ordinator, SLT ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

8.5. ICT technicians undertake half termly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

8.6. Requests regarding making changes to the filtering system are directed to the SLT and Subject co-ordinator.

8.7. Any changes made to the system are recorded by ICT technicians.

8.8. Reports of inappropriate websites or materials are made to an ICT technician immediately, who investigates the matter and makes any necessary changes.

8.9. Deliberate breaches of the filtering system are reported to the subject coordinator and ICT technicians, who will escalate the matter appropriately.

8.10. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

8.11. If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

8.12. The school's network and school-owned devices are appropriately monitored.

8.13. All users of the network and school-owned devices are informed about how and why they are monitored.

8.14. Concerns identified through monitoring are reported to the subject co-ordinator who manages the situation in line with sections 15 and 16 of this policy

9. Network security

9.1. Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians.

9.2. Firewalls are switched on at all times.

9.3. ICT technicians review the firewalls on a regular basis to ensure they are running correctly, and to carry out any required updates.

9.4. Staff members report all malware and virus attacks to ICT technicians.

9.5. All members of staff have their own unique usernames and private passwords to access the school's systems.

9.6. Pupils in class year or key stage and above are provided with a class username.

9.7. Staff members are responsible for keeping their passwords private.

9.8. Users are required to lock access to devices and systems when they are not in use.

9.9. Users inform ICT technicians if they forget their login details.

9.10 All staff use encrypted flash drives

10. Emails

10.1. Access to and the use of emails is managed in line with the Data Protection Policy and the Acceptable Use Agreement.

10.2. Staff are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours.

10.3. Prior to being authorised to use the email system, staff must agree to and sign the relevant acceptable use agreement.

10.4. Any email that contains sensitive or personal information is only sent using secure and encrypted email, such as Egress.

10.5. Staff members are required to block spam and junk mail and report the matter to ICT technician.

10.6. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this.

10.7. Chain letters, spam and all other emails from unknown sources are deleted without being opened.

11. Social networking Personal use

11.1. Access to social networking sites is filtered as appropriate. (School staff are not permitted to access personal accounts from school devices.)

11.2. Staff are permitted to use personal social media during lunchtimes; however, this must be on their own devices and only in the staffroom away from pupils.

11.3. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school.

11.4. Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media.

11.5. Pupils are taught how to use social media safely and responsibly through the online safety curriculum.

11.6. Concerns regarding the online conduct of any member of the school community on social media are reported to the Headteacher or Assistant Head, in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behavioural Policy.

Use on behalf of the school

11.8. The school's official social media channels are only used for official educational or engagement purposes.

11.9. Staff members must be authorised by the headteacher to access to the school's social media accounts.

11.10. All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

11.11. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations.

12. The school website

12.1. The headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

12.2. The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

12.3. Personal information relating to staff and pupils is not published on the website.

12.4. Images and videos are only posted on the website if parents have given permission.

13. Use of school-owned devices

13.1. Staff members are issued with the following devices to assist with their work:

- Laptop

13.2. Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons. Loaned devices have settings that are in line with the DFE guidance on home use. All loaned devices are cleared by the technician on return to school

13.3. School-owned devices are used in accordance with the Device User Agreement.

13.4. Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks.

13.5. All school-owned devices are password protected.

13.6. All mobile school-owned devices are fitted with tracking software to ensure they can be retrieved if lost or stolen.

13.7. No software, apps or other programmes can be downloaded onto a device without authorisation from ICT technicians.

13.8. Staff members or pupils found to be misusing school-owned devices are disciplined in line with the Disciplinary Policy and Procedure and Behavioural Policy.

14. Use of personal devices

14.1. Pupils in Year 5/6 may bring a telephone into school. A permission form must be completed by the parent to accept the terms of conditions of mobile phones on site. Pupils are expected to hand the phone to the office staff and collect it at the end of the school day. Any pupil found to have breached this will be disciplined following the behaviour policy/anti bullying policy.

14.2. Staff members are not permitted to use their personal devices to take photos or videos of pupils.

14.3. Staff members report concerns about their colleagues' use of personal devices on the school premises to the headteacher.

14.4. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the headteacher will inform the police and action.

14.5. The headteacher may authorise the use of mobile devices by a pupil for safety or precautionary use.

14.6. Visitors to the school are informed about the school policy for the expected use of personal devices and encrypted flash drives

14.7. Any concerns about visitors' use of personal devices on the school premises are reported to the headteacher.

15. Managing reports of online safety incidents

15.1. Staff members and pupils are informed about what constitutes inappropriate online behaviour in the following ways:

- Staff training
- The online safety curriculum
- Assemblies

15.2. Concerns regarding a staff member’s online behaviour are reported to the headteacher who will act in accordance with the relevant policies.

15.3. Concerns regarding a pupil’s online behaviour are reported to the Subject coordinator who investigates concerns with relevant staff members, e.g., the headteacher and ICT technicians.

15.4. Concerns regarding a pupil’s online behaviour are dealt with in accordance with relevant policies depending on their nature, e.g., Behavioural Policy and Child Protection and Safeguarding Policy.

15.5. Where there is a concern that illegal activity has taken place, the headteacher will contact the police.

15.6. All online safety incidents and the school’s response are recorded on CPOMS

16. Responding to specific online safety concerns Cyberbullying

16.1. Cyberbullying, against both pupils and staff, is not tolerated.

16.2. Any incidents of cyberbullying are dealt with quickly and effectively whenever they occur.

16.3. The school responds to all concerns regarding online peer-on-peer abuse, whether or not the incident took place on the school premises or using schoolowned equipment.

16.4. Concerns regarding online peer-on-peer abuse are reported to the subject coordinator who will investigate the matter in line with the Child Protection and Safeguarding Policy.

16.5. Information about the school’s full response to incidents of online peer-on-peer abuse can be found in the Child Protection and Safeguarding Policy. Online hate

16.6. The school does not tolerate online hate content directed towards or posted by members of the school community.

16.7. Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved.

17. Remote learning

17.1. All staff and pupils using video communication must:

- Communicate in groups – one-to-one sessions are only carried out where necessary.
- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable ‘public’ living area within the home with an appropriate background – ‘private’ living areas within the home, such as bedrooms, are not permitted during video communication.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.

17.2. All staff and pupils using audio communication must:

- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute audio material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they can be heard.

17.3. The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g. to provide support for pupils with SEND. This will be decided and approved by the SLT, in collaboration with the SENDCO.

17.4. Pupils not using devices or software as intended will be disciplined.

17.5. The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

17.6. The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

17.7. The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

17.8. During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

17.9. The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g., anti-virus software, on devices not owned by the school.

18. Monitoring and review

18.1. The school recognises that the online world is constantly evolving; therefore, the Subject leader, ICT technician and the headteacher conduct regular lighttouch reviews of this policy to evaluate its effectiveness.

18.2. The governing board, headteacher and subject leader review this policy in full on an annual basis and following any online safety incidents.

18.3. The next scheduled review date for this policy is November 2022. Any changes made to this policy are communicated to all members of the school community.