LOVE, COURAGE & RESPECT

Learning and Achieving Through Love, Courage and Respect

BRIGHSTONE C.E.
PRIMARY SCHOOL

E-SAFETY POLICY

Date Agreed: **June 2020**

Review Date: **June 2022**

Revision No.	Date Issued	Prepared by:	Approved by:	Comment
1	6th June 2018	JW/PM	Finance	New policy drawn from the school bus template of E-Safety and Social Media policies
2	June 2020	RL / MJ	Finance	Updated

Statement of intent

At Brighstone CE Primary School, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

The aim of this policy is to ensure appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

This policy also includes the use of social media and we are committed to:

- Encouraging the responsible use of social media in support of the school's mission, values and objectives.
- Protecting our pupils from the dangers of social media.
- Preventing and avoiding damage to the reputation of the school through irresponsible use of social media.
- Protecting our staff from cyber bullying and potentially career damaging behaviour.
- Arranging e-safety meetings for parents.

Legal framework

This policy has due regard to the following legislation, including, but not limited to:

- The Human Rights Act 1998
- The Data Protection Act 1998
- **The Regulation of Investigatory Powers Act 2000**
- The Safeguarding Vulnerable Groups Act 2006
- The Education and Inspections Act 2006
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006

This policy also has regard to the following statutory guidance:

- DfE 'Keeping children safe in education' 2020

Use of the internet

- The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.
- Internet use is embedded in the statutory curriculum and therefore all pupils are entitled to use it, though there are a number of controls the school is required to implement to minimise harmful risks.
- When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:
    - Access to illegal, harmful or inappropriate images

- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

Roles and responsibilities

- It is the responsibility of all staff to be alert to possible harm to pupils or staff, due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority.
- The headteacher is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils.
- The governing body has responsibility for ensuring that this policy does not discriminate on any grounds, including but not limited to: ethnicity/national origin, culture, religion, gender, disability or sexual orientation.
- The governing body has responsibility for handling complaints regarding this policy as outlined in the school's Complaints Policy.
- The headteacher will be responsible for the day-to-day implementation and management of this Policy and procedures.
- Parents and carers will be expected to take responsibility for the social media habits of their child/children at home, and to adhere to age restrictions on social media and other websites/electronic games.
- Parents and carers will be expected to promote safe social media behaviour.
- The headteacher is responsible for ensuring that staff receive relevant training and advice e-safety as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach pupils about online safety.
- All incidents of inappropriate internet use involving pupils will be reported using MyConcern, and incidents involving staff members will be reported to the headteacher and the LADO.
- Cyber bullying incidents will be reported in accordance with the school's Anti-Bullying Policy.
- The governing body will regularly monitor the effectiveness of the e-safety provision, current issues, and review incident logs, as part of the school's duty of care.
- The governing body will evaluate and review this E-Safety Policy every two years, taking into account the latest developments in ICT and the feedback from staff/pupils.
- All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-Safety Policy.
- All staff will ensure they understand and adhere to this E-Safety Policy, which they must sign off on MyConcern.
- Pupils have explicit instruction on internet safety and proper use of ICT.
- Parents are co-responsible for and supportive of ensuring their child understands how to use computer technology and other digital devices appropriately.
- The SLT is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

- Pupils are responsible for following the school rules and are expected to follow requests from all members of staff.

E-safety control measures

Educating pupils:

- An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of the school.
- Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material.
- Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be presented in all classrooms.
- Pupils are instructed to report any suspicious use of the internet and digital devices.

Educating staff:

- All staff will undergo e-safety training on a regular basis to ensure they are aware of current e-safety issues and any changes to the provision of e-safety, as well as current developments in social media and the internet as a whole.
- All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
- All staff are aware on which sites are deemed appropriate and inappropriate.
- All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.
- Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand this E-Safety Policy.
- The use of memory sticks, pen-drives or external hard-drives will not be permitted. All electronic documents will be saved directly on the member of staff's school laptop or on the Google Drive, and the laptop will be password protected.

Internet access:

- A record will be kept by the headteacher of all pupils who are not allowed to be granted internet access.
- Members of staff monitor pupils' activity.
- Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access, certain websites, which are harmful, or use inappropriate material.
- Filtering systems will be used which are relevant to pupils' age ranges, their frequency of use of IT systems, and the proportionality of costs compared to risks.
- The governing body will ensure that use of appropriate filters and monitoring systems does not lead to "over blocking", such that there are unreasonable restrictions as to what pupils can be taught concerning online teaching and safeguarding.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the headteacher.
- All school systems will be protected by up-to-date virus software.
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.
- The master users' passwords will be available to the headteacher for regular monitoring of activity.
- Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.
- Personal use will only be monitored by the headteacher for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.

- Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only, and no personal devices.

Email and other means of communication:

- Staff and governors **must** use their school email address for school business and personal email address for their private correspondence; the two should not be mixed.
- Use of personal email to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any other pupils, staff or third parties via email, unless it is in a password protected document. The password will not be emailed; it will be conveyed over the telephone to the correct recipient. The use of SharePoint will be used wherever possible when transferring data to external parties.
- Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.
- E-communication with pupils and parents/carers will only be by email using the official school administration email address or class email addresses, or by using the Teachers 2 Parents texting system.
- All emails from teachers to parents/class groups will be approved by the headteacher prior to being sent if the nature of the communication is of a sensitive nature or has the potential to escalate.
- The headteacher will be copied into all emails to parents/class groups (either BCC or CC where appropriate).
- The use of video conferencing between staff and children is only allowed by prior agreement and ensuring that the parent/carer has granted permission, the risk assessment is adhered to, and that parents, children and staff are aware of the safeguarding risks and ground rules.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

Social media use – staff and governors

- School social media passwords are kept by headteacher and other identified staff where necessary and appropriate. The passwords must only be shared with authorised people.
- The headteacher is responsible for what is posted on the school's social media accounts, and must approve all content before it is published.
- Members of staff may not access social media during lesson time, unless it is part of a curriculum activity.
- Members of staff may use social media during their break times.
- Members of staff should avoid using social media in front of pupils.
- Members of staff should not be "friends" with parents/carers through social media, **unless the parent/carer is another member of staff or closely involved in the school as a volunteer, or the member of staff is a fellow parent.**
- Members of staff **must not** be friends with pupils or past pupils under the age of 18 on social media.
- If pupils or parents/carers attempt to "friend" or otherwise contact members of staff through social media, the headteacher should be made aware.
- Members of staff should not identify themselves as an employee of Brighstone CE Primary School on their personal social media.
- Members of staff **must not** post any content online about Brighstone CE Primary School, its staff or its pupils unless the content is already in the public domain; this includes but is not exclusive to photos and personal comments, thoughts and feelings.
- Members of staff **must not** post content online that is damaging to the school or any of its staff or pupils.
- Where members of staff use social media in a personal capacity, they should make it clear that their views are personal. They should only post comments or photos that they would be happy to be attributed to them as a teaching professional.

- Where members of staff use social media in a personal capacity, they should use the tightest privacy settings possible.
- Teachers or members of staff **must not** post any information that could identify a pupil, class or the school.
- Members of staff **must not** post anonymously or under an alias to evade the guidance given in this policy.
- Members of staff should regularly check their online presence for negative content via search engines.
- If inappropriate content is accessed online, this should be reported to the headteacher.
- Attempts to bully, coerce or manipulate members of the school community, via social media, by teachers and members of staff will be dealt with as a disciplinary matter.
- Members of staff should not leave a computer or other device logged in when they are not able to personally supervise it.
- Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal in accordance with the Code of Conduct.
- Members of staff should be aware that if their out-of-work activity brings Brighstone CE Primary School into disrepute, disciplinary action will be taken.

Social media use – pupils

- Pupils may not access social media when they are in school, unless it is part of a curriculum activity.
- Breaches of this policy by pupils will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to prosecution, or exclusion.
- Pupils **must not** attempt to “friend” or otherwise contact members of staff through social media. If attempts to contact members of staff through social media are made, they will be reported to the headteacher.
- If members of staff attempt to “friend” or otherwise contact pupils through social media, they **must be** reported to the headteacher.
- Pupils should not post anonymously or under an alias to evade the guidance given in this policy.
- Pupils **must not** post content online that is damaging to the school or any of its staff or pupils.
- Pupils must not post photos, videos or comments that include other children at the school.
- Pupils will not post anything malicious about the school or any member of the school community on social media.
- Pupils at Brighstone CE Primary School must not sign up to social media sites that have an age restriction above the pupil’s age.
- If inappropriate content is accessed online on school premises, it **must** be reported to a teacher.

Social media use – parents/carers

- Parents/carers will be responsible for ensuring that their children do not sign up to social media sites that have an age restriction above their child’s age.
- Parents/carers **must not** attempt to “friend” or otherwise contact members of staff through social media. If attempts to contact members of staff through social media are made, the headteacher will be made aware.
- If members of staff attempt to “friend” or otherwise contact parents/carers through their personal social media account, they should be reported to the headteacher.
- Parents/carers should not post anonymously or under an alias to evade the guidance given in this policy.
- Parents/carers must not post photos, videos or comments that include other children at the school.
- Parents/carers must not use social media on their own devices while helping at school or on school visits.
- Parents/carers will not post anything malicious about the school or any member of the school community on social media.

- Parents/carers will raise queries, concerns and complaints directly with the school rather than posting them on social media.
- If a parent is accused of making malicious comments about the school or a teacher on social media, the parent will be invited to a meeting with the school. If the parent has a reasonable complaint, this should be addressed through the usual complaints procedure (see Complaints Policy and Procedure) and the school will request that the offensive comments are removed. If the parent refuses, the school may report it to the social networking site or the local authority, or will seek legal advice. Comments that are threatening, abusive, racist, sexist or that could be seen as a hate crime may be reported to the police as online harassment.

Blocked content

- Inappropriate social media websites are blocked to pupils by the network's firewalls.
- Attempts to circumvent the network's firewalls will result in a ban from using school computing equipment, other than with close supervision.
- Inappropriate content which is accessed on the school computers should be reported to the headteacher so that the site can be blocked.

Be SMART online

We encourage pupils to take a SMART approach to social media behaviour:

- **Safe** – Do not give out personal information, or post photos of yourself to people you talk to online. Follow age restriction rules.
- **Meeting** – Do not meet somebody you have only met online. We encourage parents/carers to speak regularly to their children about who they are talking to online.
- **Accepting** – We advise that pupils only open emails and other forms of communication from people they already know.
- **Reliable** – We teach pupils about the dangers of believing everything they see online.
- **Tell** – We encourage pupils to tell a teacher, parent or carer if they see anything online that makes them feel uncomfortable.

Published content on the school website and images:

- The headteacher will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- Contact details on the school website will include the phone number, email and address of the school. No personal details of staff or pupils will be published.
- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will only be posted if permission from parents has been received.
- Pupils are not permitted to take or publish photos of others without permission from the individual.
- Staff are allowed to take images on school equipment. Staff **must not** take images using their personal equipment, unless authorised by SLT.
- Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

Mobile devices and hand-held computers:

- The headteacher may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.

- Pupils are not able to access the school's Wi-Fi system at any times using their mobile devices and hand-held computers.
- Personal mobile devices are not permitted to be used during school hours by pupils. Mobile phones belonging to pupils will be kept in the office throughout the day and handed back to the pupil at home time.
- Staff are permitted to use hand-held computers that have been provided by the school, though internet access may be monitored for any inappropriate use by the headteacher when using these on the school premises.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- Personal mobile devices **must not** be used to take images or videos of pupils or staff.
- The school will be especially alert to instances of cyberbullying and will treat such instances as a matter of high priority.

Virus management:

- Technical security features, such as virus software, are kept up-to-date and managed by the IT support service.
- The IT support service will ensure that the filtering of websites and downloads is up-to-date and monitored.

Cyber bullying

- For the purpose of this policy, "cyber bullying" is a form of bullying whereby an individual is the victim of harmful, upsetting or offensive posting of information or images, online.
- The school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.
- The school will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.
- Pupils will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as relationships and sex education.
- The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.
- The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-Bullying Policy.
- The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a pupil.

Reporting misuse

Misuse by pupils:

- Teachers have the power to discipline pupils who engage in misbehaviour concerning internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the headteacher.
- Any pupil who does not adhere to the rules and is found to be wilfully misusing the internet, will have a letter sent to their parents explaining the reason for suspending their internet use.
- Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the headteacher and will be issued once the pupil is on the school premises.

- Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Child Protection and Safeguarding Policy.

Misuse by staff:

- Any misuse of the internet by a member of staff should be immediately documented and reported to the headteacher.
- The headteacher will deal with such incidents in accordance with the Allegations of Abuse Against Staff Policy, and may decide to take disciplinary action against the member of staff.
- The headteacher will decide whether it is appropriate to notify the police, the LADO or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

Appendix 1

Acceptable Use Agreement of E-Safety and social media for staff and volunteers

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school can monitor my use of the ICT systems and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, iPads, email etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident that I become aware of, to the Headteacher. In the case where the Headteacher is the alleged perpetrator, I will report to the Chair of Governors. The matter will then be referred to the LADO (Local Authority Designated Officer) – see Child Protection Policy. Child protection procedures must be followed if a child is considered to be at risk of harm: see policy. The school has a whistleblowing policy and procedure which is available via the school website.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's or pupil's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images *(an up to date list of permissions can be gained from the school office).* I will not use my personal equipment (e.g. mobile phone cameras) to record these images, unless I have the permission from the SLT to do so. Where these images are published (e.g. on the school website/Facebook) it will not be possible to identify by name, or other personal information, those who are featured, unless parental permission has been granted.
- I will not use chat and social networking sites in school (including on personal mobile phones) unless in my designated lunch break, in accordance with the school's Safeguarding, E-safety and other associated policies.
- I will only communicate with pupils and parents/carers by email using the official school administration email address or class email addresses, or by using the Teachers 2 Parents texting system. I will not use my personal work email to communicate with parents. A school email address can be obtained from the headteacher if one has not already been obtained. The exception to this is if a staff member is also a Governor and sending documents etc. in this capacity. Staff should not use personal texts, personal email addresses, social networks or blog sites for communicating with pupils or parents. The school text system is in place to contact parents if required. This is monitored on a daily basis.

- I will not engage in any on-line activity that may compromise my professional responsibilities. <u>This includes sending malicious emails and leaving any remarks about the school or my feelings towards it or other members of staff, on social network and blog sites</u>. Doing so could result in the school taking disciplinary or if necessary, police/legal action.

The school, internet provider and Diocese have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my PC/iPad/tablet/laptop/mobile phone etc... in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses prior to use.
- I will save all work on my school laptop or Google Drive (protected by a password), not on a memory stick or external hard drive.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials that are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate, or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, without the permission of the Headteacher.
- I will not disable or wilfully cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about others, or myself as outlined in GDPR. Where pupil level data is transferred outside the secure school network, it must be encrypted/password protected, or transferred via SharePoint.
- I understand that GDPR requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority i.e. Children's Services – Child Protection.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school-sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this E-Safety Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this E-Safety Policy Agreement, I could be subject to disciplinary action, in accordance with the school policy. This could include a warning, a suspension,

referral to Governors and/or the Local Authority and in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: ____

Signed: ________________________________

Date: __________________________________