Broad Chalke CE VA Primary School

Online Safety and Responsible Use Policy

Mission Statement: With the love of God we learn, care, grow and share

We believe in the educational benefits of Digital Technology for effective teaching and learning. Secure and effective internet access for pupils should be seen as an entitlement on the basis of educational need and an essential resource for staff. This document was written with the following key principles in mind:-

- All users are protected from inappropriate material, bullying and harassment
- Users have access to resources to support learning and teaching
- Users should be given clear boundaries on responsible and professional use

1. Leadership and Management

1.1 Developing a policy

Our Online Safety and Responsible Use policy has been written using the Wiltshire template policy and government guidance. It will be reviewed annually by the subject leader, shared with staff and approved by governors. This policy has also been shared with our online safety committee of pupils,

1.2 Authorised Access

- Parents will be informed that pupils will be provided with supervised Internet access and they sign a form to acknowledge this as part of their starter pack.
- We receive Internet Service Provision (ISP) from South West Grid for Learning (SWGfL) and have a service which proactively monitors Internet usage for attempts to access illegal content and will notify the local police and Wiltshire Council in these instances.
- We keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date; for instance if a pupil's access is withdrawn. Pupils sign a responsible use agreement and adults sign to say they have read this policy. Any adult / parent helpers will also be given this policy and asked to sign to say they have read it and will abide by it.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials wherever possible.

1.3 Filtering and Monitoring

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Levels of access and supervision will vary according to the pupil's age and experience. Internet access must be appropriate for all members of the school community from the youngest pupil to staff.

- A log of all staff with access to the Internet will be kept and regularly reviewed.
- A designated member of staff (the School Business Manager) has the authority to review popular, permitted and banned sites accessed in school.
- We work in partnership with parents, Wiltshire Council, DFE and our ISP, to ensure systems to protect pupils are reviewed and improved.
- If unsuitable sites are discovered, the web address and content must be reported to the ISP via the School Business Manager.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that we believe is illegal or may place an individual at risk will be referred to the appropriate authorities i.e. Head teacher, DOFA (Designated Officer for Allegations), Police, Internet Watch Foundation.

1.4 Risk Assessment

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. We will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not

possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Wiltshire Council can accept liability for the material accessed, or any consequences of Internet access.

- Methods to identify, assess and minimise risks will be reviewed regularly.
- The head teacher will ensure that the Internet policy is implemented and compliance with the policy monitored.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

2. Teaching and Learning

2.1 The Curriculum

The Internet is an essential resource to support teaching and learning. The statutory curriculum requires pupils to be responsible, competent, confident and creative users of information and communication technology. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources, e-mail and mobile learning. Computer skills are vital to access life-long learning and employment; ICT is an essential life-skill.

- The Internet is an essential part of everyday life for education, business and social interaction
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement and wellbeing, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Whilst Internet access is an entitlement, users will need to show a responsible and mature approach to its use or this privilege may be removed.
- 'Swiggle' or 'Safesearch' can be used instead of Google for online information, searches or images. However, this does limit search results and this does not teach pupils what to do should they come across something inappropriate. We feel it is important to teach children how to use Google appropriately.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

2.2 Enhancing Teaching and Learning

Benefits of using the Internet in education include:

- Access to a variety of worldwide educational resources.
- Educational and cultural exchanges between pupils worldwide.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments.
- Educational materials and effective curriculum practice.
- Collaboration across networks of schools, support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Access to learning wherever and whenever convenient.

2.3 Evaluating Content

Information received via the web, e-mail or text message requires good information-handling and digital literacy skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues may be missing or difficult to read.

Ideally inappropriate material would not be visible to pupils using the web but this is not easy to achieve and cannot be guaranteed. Pupils are taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

- Pupils will be taught to be critically aware of the materials they read and how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.

- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- If staff or pupils discover an unsuitable site or content they consider to be inappropriate, the URL (address) and content should be reported to their ISP/SWGfL via the School Business Manager. A record is made by the member of staff in the online safety folder and procedures followed in line with our flow chart. If a pupil has been affected the Headteacher will inform the parents.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to acknowledge the source of information used and to respect individuals and intellectual property when using Internet material in their own work.

3. Communication and Content

3.1 Website Content

- The point of contact on the school website should be the school address, school e-mail and telephone number. Staff or pupils' personal information will not be published.
- Written permission from individuals, parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- The nature of all items uploaded will not include content that allows the pupils to be identified, either individually or through aggregated pieces of information.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

3.2 Learning Platforms

At this stage we do not have a Learning Platform.

3.3 Managing e-mail

The use of e-mail requires appropriate safety measures.

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a responsible adult if they receive offensive e-mail.
- Pupils should use email in an acceptable way. Sending images without consent, explicit images, messages that cause distress and harassment to others are considered significant breaches of this school policy and will be dealt with accordingly.
- E-mail sent to an external organisation should be written carefully and where appropriate, authorised before sending, in the same way as a letter written on school headed paper.

3.4 On-line communications and Social Media.

On-line communications, social networking and social media services will be filtered in school by the ISP but are likely to be accessible from home.

All staff must be aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. Staff must be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. Schools have a key role to teach young people about the importance of how to communicate safely and respectfully online, keeping personal information private.

- There is an official school Instagram account, approved by governors and operated strictly in line with the School Social Media Policy.
- Staff and pupils will be taught about how to keep personal information safe when using online services. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff official blogs or wikis should be password protected and only operate with approval from the SLT.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- No member of the school community should publish specific and detailed private thoughts about the school, especially those that may be considered threatening, hurtful or defamatory.
- Parents wishing to photograph or video at an event should be made aware of the schools expectations with regard to sharing these images online i.e. out of politeness and consideration, parents are asked not to put photos of other people's children on social media sites without the permission of those parents.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction.
- In line with, 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' it will not be considered appropriate for staff to engage in personal online communications with children and young people. Express care is also to be taken regarding the use of social networking sites.

3.5 Mobile Devices (Including Bring You Own Device-BYOD)

Mobile devices refers to any device that provides access to the internet or internal network for example, tablet (Apple, Android, Windows, and other operating systems) e-readers, mobile phone, iPad, iPod touch, digital cameras. Our general policy is that pupils are NOT allowed to bring their own device to use in school unless permission has been given for a specific occasion e.g. a smart phone with camera for a trip. However, members of staff are permitted to bring and use their own devices for educational use. On those occasions when mobile devices are allowed the following will apply:-

- Mobile devices that are brought in to school remain the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items.
- School staff authorised by the Head teacher may search pupils or their possessions, and confiscate any mobile device they believe is being used to contravene school policy, constitutes a prohibited item, is considered harmful, or detrimental to school discipline. If it is suspected that the material contained on the mobile device relates to a criminal offence, the device will be handed over to the Police for investigation.
- Sending abusive or inappropriate messages or content is forbidden by any user within the school community.
- Mobile devices may be used during lessons or formal school time as part of approved and directed curriculum based activity.
- Mobile devices are not permitted to be used in certain areas or situations within the school site e.g. changing rooms or toilets, situations of emotional distress etc.
- Where staff may need to contact children, young people and their families within or outside of the setting in a professional capacity, they should only do so via an approved school account (e.g. E-mail, phone, social media) In exceptional circumstances there may be a need to use their own personal devices and account; this should be notified to a senior member of staff ASAP.
- Staff should be provided with school equipment for the taking photos or videos of pupils linked to an educational intention. In exceptional circumstances staff may need to use personal devices for such a purpose and when doing so, should ensure they comply with this policy.
- Any images taken using personal devices must be saved to the school network and the image deleted from the personal device and any cloud storage as soon as possible.
- For the safeguarding of all involved, users are encouraged to connect mobile devices through the school wireless provision and service that allows the ability to filter any device that uses the school Internet connection, without having to configure the user's device.

- We will take steps to monitor responsible use in accordance with this policy.

3.6 Video Conferencing

- We do not currently have video conferencing facilities in school.
- Staff must refer to this policy prior to children taking part in video conferences.
- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Video conferencing will be supervised appropriately for the pupil's age and ability.

3.7 Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

3.8 Cyber Bullying or Online Bullying

Cyber bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet, to deliberately hurt or upset someone" DCSF 2007.

For most, using the internet and mobile devices is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that young people, school staff, parents and carers understand how cyber bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety. Teaching pupils how to deal with cyber bullying is part of our online safety curriculum.

Cyber bullying (along with all other forms of bullying) of or by any member of our school community will not be tolerated. Full details are set out in the school's behaviour, anti-bullying and child protection policies, which include:

- Clear procedures set out to investigate incidents or allegations of cyber bullying.
- Clear procedures in place to support anyone in the school community affected by cyber bullying.
- All incidents of cyber bullying reported to the school will be recorded.
- We will take steps to identify the bully, where possible and appropriate. This may include identifying and interviewing possible witnesses, and contacting the ISP and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyber bullying and the school's online safety ethos.

3.9 Data Protection

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the forthcoming GDPR May 2018.

4 Implementation

4.1 Policy in Practice - Pupils

Many pupils are very familiar with Internet use and the culture that surrounds it. As part of our online safety teaching and awareness-raising we discuss the key features with pupils / students as appropriate for their age.

- All users will be informed that network and Internet use will be monitored.
- Online Safety teaching is integral to the curriculum and raises the awareness and importance of safe and responsible internet use amongst pupils.
- Online Safety teaching is included in PSHE, Citizenship and/or ICT and covers safe use at school and home.
- Online Safety rules and/or copies of the Responsible Use Policy for pupils are on display in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

4.2 Policy in Practice - Staff

It is important that all staff feel confident to use new technologies in teaching and our Online Safety Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. Particular consideration must be given when members of staff are provided with devices by the school which may be accessed outside the school network. Schools must be clear about the safe and appropriate uses of their school provided equipment and have rules in place about use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of school information. If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with their senior leader to avoid any possible misunderstanding.

- The Online Safety and Responsible Use Policy will be provided to all members of staff and any adult or parent helpers who may use school IT equipment. A form will be signed to acknowledge it has been read and that staff agree to comply.
- Staff should be aware that Internet traffic is monitored (and automatically reported by the SWGfL) and can be traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff and governors on an annual basis.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

4.3 Policy in Practice - Parents

Parents need to be aware of the potential dangers that are associated with online communications, social networking sites and mobile technologies to help ensure their children are not putting themselves at risk. We refer parents to suitable educational websites via our school website.

- Parents' attention will be drawn to Online safety through the Responsible Use of ICT and the Internet agreement in the school's new parent welcome pack, newsletters and the school Website.
- A partnership approach with parents will be encouraged. We offer parent evenings, practical sessions and suggestions for resources and safer Internet use at home.
- Regular information is provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.
- Internet issues will be handled sensitively to inform parents without undue alarm.

4.4 Handling of complaints

Parents and teachers must know how and where to report incidents in line with the school complaints policy and complaints of a child protection nature must be dealt with in accordance with the LA Child Protection procedures. Prompt action will be required if a complaint is made. The facts of the case will need to be established; for instance whether the Internet use was within or outside school. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's behaviour policy. All records of the incident should be kept, e.g. e-mails saved or printed text messages saved etc.

- Responsibility for handling incidents is delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

Ratified by FGB: January 2014
Reviewed: January 2015, January 2016, January 2017, January 2018
Next review due: January 2019

Policies to be read in conjunction with this policy: Behaviour, Anti-Bullying, Personal, Social and Health Education (PSHE), Child Protection, School Social Media Policy, Data Protection and Staff Code of Conduct for Safer Working Practice.