BROADWATER
CHURCH OF ENGLAND
PRIMARY SCHOOL

Rectory Gardens
Worthing
West Sussex
BN14 7TQ

TEL 01903 235389
EMAIL office@broadwaterce.org

Headteacher: Mrs N Simpson

www.broadwater.w-sussex.sch.uk

E-Safety Policy
2022-2025

Turn your ear to wisdom and apply your heart to understanding (Proverbs 2:2)

Broadwater is a Christian School. We will enable children to become wise, confident, successful learners with the motivation, skills and responsibility to make a positive difference in God's world. Our vision is underpinned by the values we live by.

The Holy Spirit produces this kind of fruit in our lives: love, joy, peace, patience, kindness, goodness, faithfulness, gentleness, and self-control. There is no law against these things! Galatians 5:22

It is this fruit that, in partnership with parents, we will instil in the children of our school.

The school's e-safety policy will operate in conjunction with other policies including:

- Pupil Behaviour
- Anti-Bullying
- Safeguarding and Child Protection
- RHE Policy
- RSE Policy
- All Online Safety Policies
- Data Protection and Security

What is E-safety?

E-Safety encompasses the use of new technologies, internet and electronic communications such as: mobile phones, collaboration tools and personal publishing. E-safety concerns safeguarding children and young people in the digital worlds. It emphasises learning to understand and use new technologies in a positive way, about the risks and the benefits. E-safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.
E-Safety depends on effective practice at a number of levels:

• Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
• Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
• Safe and secure broadband including the effective management of filtering.
• A member of staff being responsible for the implementation and monitoring of this e-safety policy.

Introduction

The purpose of this policy is to:

- Through consultation with pupils establish the ground rules we have in Broadwater Church of England Primary School for using the Internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience, appropriately.
- Describe how these fit into the wider context of our discipline and RHE and RSE policies.
- Demonstrate the methods used to protect children from sites containing pornography, racist or politically extreme views and violence.
- Understand that accessing inappropriate sites accidentally is not something to feel guilty about and that any such incident should be reported to staff immediately.

Teaching and learning

- 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.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.

- Pupils are taught what Internet and social media use is acceptable and what is not and given clear objectives for Internet use.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school ensures that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- A planned online safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and in class activities
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. *N.B. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.*

Managing Internet Access

- School ICT systems capacity and security is reviewed regularly.
- Virus protection is updated regularly (JSPC).

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive or inappropriate e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- E-mail sent to an external organisation must be authorised before sending, in the same way as a letter written on school headed paper.

School web site

- The contact details on the school web site should be the school address, e-mail and telephone number. Staff or pupils' personal information is not published.
- The head teacher has overall editorial responsibility and ensures that content is accurate and appropriate.
- Photographs that include pupils are selected carefully so they do not enable individual pupils to be clearly identified, unless parental permission has been given.
- Pupils' full names are not used anywhere on the web site blog or Twitter.
- Written permission from parents or carers must be obtained before photographs of pupils are published on the school web site.
- Pupil's work will only be published with the permission of the pupil and parents.

Social networking and personal publishing

- The school blocks access to social networking sites.
- Newsgroups are also blocked.

- Pupils are told never to give out personal details of any kind which may identify them.
- Pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

- If staff or pupils discover an unsuitable site, it must be reported immediately to the e-Safety Coordinator/ ICT technician (JSPC).
- Senior staff ensures that regular checks are made to ensure that the filtering methods are appropriate and effective (JSPC).

Managing emerging technologies

- Emerging technologies are examined for educational benefit and a risk assessment is carried out before use in school is allowed.
- Mobile phones are not used during lessons or formal school time. Any mobile phone brought into school by a child for a specific purpose remains the sole responsibility of that child (Yr5/6 only). The school takes no responsibility for the loss or damage of that phone. The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

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

Policy decisions

Authorising Internet access

- All staff are expected to adhere to 'Acceptable ICT Use Agreement' before using any school ICT resource.
- All pupils in the school are expected to adhere to an acceptable use policy when they join the school, and on commencement of a new Key Stage (Key Stages 2).
- Early Years and Key Stage 1, access to the Internet will be closely supervised by an adult, with access to specific, approved on-line materials.
- At Key Stage 2, access to the Internet will be by supervised access to specific, approved on-line materials.

Assessing risks

- The school takes all reasonable precautions to ensure that user's access only appropriate material by using West Sussex's filtering system.
- The school audits ICT provision on an annual basis to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse are dealt with by a senior member of staff.
- Any complaint about staff misuse is referred to the headteacher.
- Complaints of a child protection nature are dealt with in accordance with the school's child protection procedures.
- Pupils and parents are informed of the complaint's procedure.

In the event of suspicion, all steps in this procedure should be followed: (See Online Safety Policy.)

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
- Internal response or discipline procedures
- Involvement by Local Authority or national/local organisation (as relevant).
- Police involvement and/or action

- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - promotion of terrorism or extremism
  - offences under the Computer Misuse Act (see User Actions chart above)
  - other criminal conduct, activity or materials

- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Communications

Introducing the e-safety policy to pupils

- E-safety rules are posted in all networked rooms and discussed with the pupils at the start of each year *(see Appendix 3 for Internet Safety Rules)*.
- Pupils are informed that network and Internet use will be monitored.
- As part of the National Curriculum and skills development, Key Stage 2 pupils and their parents are informed of the child exploitation and online protection centre: www.thinkuknow.co.uk

Staff and the e-Safety policy

- All staff have copies of the school's e-Safety Policy and know its importance.
- Staff are aware that Internet traffic can be monitored and traced to the individual user.

Enlisting parents' support

- Parents' attention is drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school Web site.

Cyber Bullying

What is cyber bullying?

- Cyber bullying includes sending or posting harmful or upsetting text, images or other messages, using the internet, mobile phones or other communication technology.
- It can take many forms, but can go even further than face to face bullying by invading home and personal space and can target one or more people.
- It can take place across age groups and target pupils, staff and others.
- It can include threats and intimidation, harassment, defamation, exclusion or peer rejection, impersonation and unauthorised publication of private information or images.
- It can include messages intended as jokes, but which have a harmful or upsetting effect.

Cyber bullying may be carried out in many ways, including:

- Threatening, intimidating or upsetting text messages;
- Threatening or embarrassing pictures and video clips via mobile phone cameras;
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible;
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name;
- Menacing or upsetting responses to someone in a chat-room;
- Unpleasant messages sent during instant messaging;
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites

In some cases, this type of bullying can be a criminal offence.

Responding to cyber bullying

Cyber bullying will generally be dealt with through the schools Anti-Bullying Policy. A cyber bullying incident might include features different to other forms of bullying, prompting a particular response. Key differences might be:

- Impact: possibly extensive scale and scope
- Location: the anytime and anywhere nature of cyber bullying
- Anonymity: the person being bullied might not know who the perpetrator is
- Motivation: the perpetrator might not realise that his/her actions are bullying
- Evidence: the subject of the bullying will have evidence of what happened

Investigation

- Again, the nature of any investigation will depend on the circumstances. It may include, for example,
- Review of evidence and advice to preserve it, for example by saving or printing (e.g. phone messages, texts, emails, website pages)
- Efforts to identify the perpetrator, which may include looking at the media, systems and sites used. Witnesses may have useful information.
- Contact with the Internet Watch Foundation, the police or the Safeguarding Children Board Officer if images might be illegal or raise child protection issues

- Requesting a pupil to reveal a message or other phone content or confiscating a phone. Staff do not have the authority to search the contents of a phone.

This policy will be reviewed, annually, by the subject leader for computing in the light of new guidance and presented to staff and governors.

Cyber Safety Code

Three Steps to Safety

1. Respect other people - online and off. Don't spread rumours about people or share their secrets, including phone numbers or passwords.
2. If someone insults you online or by phone, stay calm. Ignore them, but tell someone you trust.
3. "Do as you would be done by!" Think how you would feel if you were bullied. You are responsible for your behaviour - so don't distress other people or encourage others to do so.

If you are being bullied

It is never your fault. It can be stopped and it can usually be traced.

- Don't ignore the bullying. Don't reply, but do tell someone you can trust, such as a teacher or parent, or call an advice line.
- Try to keep calm. If you seem frightened or angry it will only make the person bullying you more likely to continue.

Text / video messaging

- You can turn off incoming messages for a couple of days.
- If bullying persists you can change your number (ask your mobile phone provider).
- Do not reply to abusive or worrying messages. You can report them to you mobile phone provider.

Email

- Never reply to unpleasant or unwanted messages.
- Don't accept emails or open files from people you don't know.
- Don't delete bullying emails – print them or save them as evidence in a separate folder.

Social networking sites, chatrooms and instant messaging

- Change privacy settings so you can choose who to be friends with and who can see your profile. Don't add anyone you don't know to your friend list.
- Don't use your real name in chatrooms.
- Never give out your photo or personal details, like your address, phone number or which school you go to.
- Don't post any pictures or videos you wouldn't be happy for your parents or teachers to see. Once they are online they can be copied and posted in other places where you can't get rid of them.
- Keep your passwords private and don't tell anyone, not even your best friend.
- To report suspicious behaviour online and to learn more about keeping yourself safe online visit www.thinkyouknow.co.uk

Always report bullying incidents.
Not doing that allows the bully to continue.
That's not good for the victims, for those who witness the incidents or for the bully, who may need help to change their antisocial behaviour.

KEY STAGE 1

These rules help us to stay
safe on the Internet

Think then Click

We only use the Internet when an adult is with us.

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Key Stage 2

Think then Click

We ask permission before using the Internet.

We only use websites our teacher has chosen.

We immediately close any webpage we don't like.

We only e-mail people our teacher has approved.

We send e-mails that are polite and friendly.

We never give out a home address or phone number.

We never arrange to meet anyone we don't know.

We never open e-mails sent by anyone we don't know.

We never use Internet chat rooms.

We tell the teacher if we see anything we are unhappy with.

J. Barrett & H. Barton