Beachborough School

Online (E-Safety) Policy

Updated: September 2022

Date of next Review: September 2023

Policy Lead: Susi Blithe (Head of Computing) & Mr S Preece (Deputy Headmaster - DSL)

Reviewed by: Senior Leadership Group

Beachborough aims to:

- Ensure secure and supervised access to information and communication technology (ICT) for all pupils
- Encourage pupils to use technology to support their learning
- Promote the notion of Digital Health and Safety
- Encourage all members of the community to gain a healthy balance of ICT use in both school and at home.

Beachborough recognises the importance of mobile devices and computers for communication and education as well as for recreation and socialising. However, we also recognise that some individuals may use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to grooming and enticing children to engage in sexually harmful conversations, webcam photography or face-to-face meetings. Students may also be distressed or harmed by accessing inappropriate websites that promote unhealthy lifestyles, extremist behaviour and criminal activity. Abuse can take place wholly online and may be used to facilitate offline abuse. Children may also use these technologies in a way that leaves them vulnerable.

Beachborough educates pupils about e-safety issues across all curriculum subjects, but particularly in the following ways:

- PSHE lessons
- Computing lessons
- Age-specific assemblies

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers a school to protect and educate pupils in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into **four areas of risk**:

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non- consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying).

Commerce: - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Filters and Monitoring

The Governing Body has done all it can reasonably do to limit children's exposure to the risks described above. The school has safeguarding and filtering systems in place with active monitoring to help create a safe online environment for our pupils. Children are currently not allowed to bring mobile technology into school unless with the permission of the Head of Learning Support to support learning, for children with LDD/SEN. Children do not have access to the wifi code and there is a poor 3G/4G/5G currently available on site. A suitable risk assessment for filters has been completed in fulfilling the school's 'Prevent Duty' and the school acknowledges guidance is available from the UK Safer Internet Centre. The Governors are mindful of 'over-blocking' due to filters and monitoring systems. The DSL meets monthly with the ICT manager on matters of online and digital safety, reviewing the effectiveness of filters and monitoring systems.

Education
The Computing and PSHE schemes of work details how the school builds resilience in our pupils to protect themselves and their peers through education and information. Our approach to online safety empowers all staff to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate. Further guidance on 'education' should be directed to Mrs. S. Blithe and Mrs. C. Harrison.

Reporting E-Safety Concerns
Any pupil, member of staff or parent who has an e-safety concern should in the first instance refer it to the Designated Safeguarding Lead, who will take any necessary action in line with the school's Safeguarding Policy. This might include reporting concerns to the police or ESAS.

Where the concerns are not of a safeguarding nature, the issue will be referred to the appropriate pastoral team within the school.

Social networking and other inappropriate sites are blocked and monitored by the school web filtering system to ensure we are compliant with the regulations stipulated in KCSIE 2022.

However, the school realises many pupils have access to these sites outside of school. Pupils are reminded that regardless of where their posting originates, any posting of comments, photographs or videos to these sites, YouTube or similar sites which would be derogatory to the school or the school community, or threaten, demean, or bully members of staff or other pupils, is strictly prohibited and may result in disciplinary action being taken by the school.

Responsibilities
- Mr. S. Preece is our Whole School Deputy Head and Designated Safeguarding (and Prevent) Lead for child protection. He will listen and take you seriously if you are concerned about anything to do with e-safety, including concerns you may have about another pupil.
- Mrs. S. Blithe is our Head of Computing and Deputy DSL. She will require all pupils to understand the Acceptable Usage Policy which they agree to when accessing the computers in the computer suites.
- Questions regarding our technical provision/infrastructure and the safeguards in place to filter and monitor inappropriate content should be directed to the IT Manager. He will alert the DSL (and the headmaster) to any safeguarding issues.
- Mrs. C. Wallace is our Bursar. She is our Data Protection Co-ordinator who will endeavour to ensure that all personal data is processed in compliance with regulatory requirements.

Prevent Duty
- The school delivers a proportionate response with respect to a duty to prevent pupils becoming extremist or radicalised.
- It is recognised that both encouraging extremism and radicalism is a form of child abuse and all staff must treat suspicions as they would any other form of child abuse.
- Evidence suggests that social media is the greatest method used by those who wish to encouraging extremism and radicalism. The Home Office and DfE have produced a useful paper titled: 'How Social Media Is Used to Encourage Travel to Syria and Iraq' It can be found here: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/440450/How_social_media_is_used_to_encourage_travel_to_Syria_and_Iraq.pdf
- Additional guidance can be found here: www.saferinternet.org.uk www.thinkuknow.co.uk

This policy applies across the whole school including Boarding and EYFS and will be reviewed and updated regularly. ***Linked Policies and read in conjunction with:*** *Safeguarding, Behaviour, Taking and Use of images, Social Media, Anti-bullying, Equal Opportunities, Boarding, Staff Code of Conduct.*

Appendix 1:

Dear Parents,

<u>Guidelines for Beachborough Pupils Using the School Network, Email and the Internet. Acceptable Usage Agreement.</u>

We provide guidelines for pupils who are using the school network, email and the internet and the pupils are regularly reminded of their responsibilities when using this system. We would be very grateful if you could read the guidelines below with your child and then sign to agree to the school's acceptable usage policy.

The school will provide a filtered email and internet access service and will record and monitor all use of the system. These guidelines should help you to use the school network, email and the internet safely and responsibly. **Normal school rules for behaviour apply.**

A pupil's use of email and the internet should be guided and controlled in the same way as other information sources such as television, telephones, films, radios and other potentially offensive media. At school, staff will guide pupils. Outside of school, families bear responsibility for such guidance.

Username and Password:

- You must never share your passwords or give access to your Beachborough systems to anyone else.
- Use of another person's network account is forbidden.
- Users must not walk away and leave their computer logged on.

Network:

- Users should not send or take part in writing any text, or prepare any graphics, or create audio/video material which may be unkind, offensive, abusive, obscene or defamatory; this would be treated as cyber-bullying and is against the law. If you find any material of this nature, you must report it immediately.
- A user's files are not private. If we think they pose a risk to the system in any way or if any misuse is.
- suspected, these files may be examined and, if necessary, deleted.
- Software programmes or games must not be downloaded, saved to the network or installed.
- If you need to copy work from your own removable media, please see the Head of Computing/IT Manager.

Email:

- Whilst at school, you can only use Beachborough email server and your own address.
- Whilst you are at school, you may only send emails externally to members of your family and friends whilst boarding whilst under supervision.
- You are not permitted to send emails to ***any other pupil at Beachborough via Beachborough email system***, either internally or from a computer at home. If you want to contact another pupil, speak to them directly. This is not intended to prevent you from contacting your friends at any time, it's just that email or messaging systems are often not the best way of doing this. Try to communicate face-to-face whenever possible.
- You must never send an email that contains ***rude, abusive or offensive language***. Emails containing such language are captured and stored. They form part of your record at Beachborough.
- If you receive an email which makes you feel uncomfortable in any way (for example, if it is from someone you don't know or if it contains offensive language or pictures), you must tell a trusted adult immediately. If you are in school, tell a member of staff or go to the Head of Computing for help.

The Internet:

- Think very hard about the personal information you give out online. If you are being asked to give out personally identifiable information (like your birthday or real name), ask a teacher or a trusted adult before you do so.
- You should realise the potential dangers of corresponding with unknown people by email or through internet sites. You should never give out details which would enable them to identify and locate you.
- Do not believe everything you read on the Internet. Even trusted sources can be wrong.
- Copying and pasting is not good. Do not copy things from websites (or books) unless you have been told to by your teacher. Do not try to claim work, which is not yours, as your own. This is serious and you need to understand this fully before you leave Beachborough.
- You must never attempt to deliberately search for any information that might contain rude, offensive, or abusive, language or pictures.
- Do not sign up to any chat, email groups or social networking sites (e.g. Facebook, Instagram, Snapchat, Tik Tok etc.) until you are old enough to legally do so. Social media is not allowed at school.
- Do not request further information from any person, company or organisation using your school email address.
- Do not use sites that contain chat, chat rooms or forums of any kind.
- If you find or see a website that makes you feel uncomfortable or scares you, please tell a member of staff.
- You must not access any games sites during lessons unless a member of staff has asked you to do so.
- Give yourself a break. Don't stay online too long. Spend time with your friends and family offline.
- Teach your teachers and parents. Spend time teaching your teachers and parents about your online activities. Show them your favourite websites and explain how you are making good use of the Internet

Teams:

Whilst engaging with peers and teachers using Microsoft Teams, pupils are reminded to:

- Adhere to the school's normal expectations on behaviour and appropriate language during the sessions.
- Report any instance of inappropriate behaviour to a parent / responsible adult and appropriate member of the Senior Leadership Team.
- Be aware that when working on Microsoft Teams, sessions may be remotely monitored by other members of staff.
- Only contact teachers using Microsoft Teams or via parents, using school email addresses.
- Beachborough pupils may only use the Chat function within Teams to speak to members of staff not fellow pupils.

Live Audio / Video communication:

- In the event of a school closure we may implement the live audio / video communication functionality of Microsoft Teams. In addition to the above guidance, pupils and parents are informed of the following expectations during any such communication.
- Pupils must make sure they are dressed appropriately for and audio / video online sessions.
- Pupils should join virtual sessions from a common area in their house whereby parents and responsible adults can easily supervise sessions. Pupils are not to be in a separate room alone, for example, in their bedroom.

Monitoring:

- Beachborough monitors all internal computer and Beachborough laptop use.
- Beachborough is alerted to content which is deemed inappropriate or where there is a safeguarding concern for the welfare of the pupil.
- Any concerns logged will be followed up by an appropriate member of staff.

Reporting:

- If you see something that makes you feel uncomfortable, then please tell a trusted adult as soon as you can. If you're not sure whether the thing you see is illegal, ask the person about it when you tell them.
- If you are being cyber-bullied or harassed in any way, you should tell a trusted adult as soon as you can. If you are not comfortable telling someone you know, you can contact Childline at http://www.childline.org.uk or 0800 1111.

Sanctions:

- Any pupil found behaving irresponsibly or inappropriately and not complying with these guidelines will be reported to the appropriate member of staff.
- Beachborough reserves the right to sanction pupils for actions taken outside of school which have an impact on those within. Likewise, pupils will be sanctioned for anything which affects the reputation of Beachborough.
- The school has the right to restrict a pupil's use of the internet.

Just Remember…

If you are ever in doubt, unsettled by what you see, feel uncomfortable or if you think there is a problem, please ask a trusted adult or member of staff for advice. We will always do our best to help you.

If you are worried about something and you would like to tell someone without talking face-to-face, please email Mrs Blithe' Head of Computing: scb@beachborough.com or Mr Preece, Deputy Headmaster: s.preece@beachborough.com and they will get back to you as soon as they can. Please remember that all network, email and Internet usage at Beachborough is recorded and monitored.

For further information please contact one of the following members of staff –

- Mrs Blithe, Head of Computing
- Mr Preece, Deputy Headmaster
- Mr Rodd, IT Manager

Acceptable Use of Information and Communications Technology

Name of Pupil: - _____

As the parent or legal guardian of the pupil signing above, I grant permission for my child to use email and the Internet at school.

I understand that pupils will be held accountable for their own actions.

I have read through the Guidelines for **Beachborough Pupils Using The School Network, Email and the Internet** with my child.

I understand that although access will be through a filtered service it may be possible that some of the material accessible may be objectionable. I accept responsibility for setting standards for my child to follow when using, selecting, sharing and exploring information and media in line with school expectations.

Name of Parent: -_____

Date signed: -_____