Quality First Education Trust

Online Safety Policy

Last review: July 2019
Date of next scheduled review: July 2020

SAFEGUARDING AND PROMOTING THE WELFARE OF CHILDREN IS EVERYONE'S RESPONSIBILITY

This policy is to be considered in conjunction with the following Quality First Education Trust policies:

- Safeguarding and Child Protection Policy
- ICT Acceptable Use Policy
- Data Protection Policy

It will also operate alongside other Trust and school policies which look at keeping children safe online, such as ICT curriculum, behaviour and anti-bullying policies.

The policy and its implementation will be reviewed annually by local governors and Trustees. All staff are required to read it.

School-specific online safety information				
School name	Belleville Primary School	Belleville Wix Academy	The Alton Primary School	Churchfields Primary School
Online safety coordinator	Samantha Burst	Luke Redman	Naheed Bashir	Liz Williams

CONTENTS

1. Introduction

Online safety encompasses internet technologies and electronic communications such as mobile phones as well as 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. A whole school approach to online safety is essential to safeguarding children. It's not the job of one person and it is definitely not just a technical solution.

This policy has been written in line with the statutory guidance for schools 'Keeping Children Safe in Education'.2019 The policy and its implementation will be reviewed annually. It is available to all staff and is available on the Trust and school websites.

An **online safety co-ordinator** is named in the safeguarding annexe (Schedule 1) for each school in the Trust.

2. Why online activity is important in school

The internet is an essential element for education and social interaction in 21st Century life.

- Our schools have a duty to provide children 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 children.
- It is important that children become familiar with Information and Communication Technology (ICT) at an early age, to develop the skills they will need for the remainder of their education and in adult life. ICT enables learners to participate more readily in a rapidly changing world.
- ICT can help engage, motivate and stimulate children, and help them access new ideas and experiences. We use technology to support lessons in subjects across the curriculum.
- Effective use of the internet will enhance learning. Children learn how to use the internet in research, including the skills of knowledge location, retrieval and evaluation. Children are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

3. Internet safety

- We acknowledge that, as well as providing a variety of positive opportunities, the use of technology has become a significant component of many safeguarding issues, and can provide the platform that facilitates exploitation of children and young people. The breadth of issues classified within online safety are considerable but can be classified into three areas of risk:
    - Content: being exposed to illegal, inappropriate or harmful material
    - Contact: being subjected to harmful online interaction with other users
    - Conduct: personal online behaviour that increases the likelihood of, or causes harm, such as the sending of explicit images or online bullying.
- This includes use of computers, iPads and mobile phones.

- This includes dangers and risks involved with online chatting, social media, sharing youth produced sexual imagery (sexting), Sextortion (the threat to reveal intimate images to get you to do something you don't want to do) grooming and gaming (including risks involved in electronic sports (ESport)
- We are aware of risks to children online and will ensure children are safeguarded in school from potentially harmful and inappropriate online material through appropriate filtering and monitoring systems.
- Internet access is filtered, to block access to unsuitable content. Senior staff will ensure that regular checks are made to ensure that filtering is appropriate, effective and reasonable.
- Internet access in lessons is managed and monitored carefully and appropriately for the age of the pupils, with clear objectives. This monitoring applies even when children undertake online research on their own or in small groups, which helps encourage them to be independent learners.

The use of any internet derived materials complies with copyright law.Pupils are taught what internet use is acceptable and what is not. If they do come across any inappropriate content they are told to report this to an appropriate member of staff.

- Children are taught how to be aware of online safety and risks and laws involved with social network sites, contacting strangers and cyber-bullying including youth produced sexual imagery (sexting), grooming, child sexual exploitation (CSE), and interaction with people during gaming and the use of mobile phones.
- We filter access to social networking sites, but may allow them for specific supervised activities.
- Children are taught that they must not reveal personal details of themselves or others online or in emails, or arrange to meet anyone without specific permission.
- ICT systems capacity and security are reviewed regularly. Virus protection, operating systems and applications are updated regularly. Security strategies are discussed with our ICT support provider. We will also work with the internet service provider to ensure appropriate systems to protect children are in place.

4. Mobile phones and email safety

- We understand that some children will bring in mobile phones, for example for parent reassurance if they are walking to and from school by themselves. However, they are required to hand in their phones to the teacher at the start of the day.
- Occasionally children may make use video conferencing technology as part of a school activity, for example to speak with children in another school or site. They may only do this with permission and supervision from a member of staff.
- Children may only use approved email accounts on the school system.
- Children must immediately tell a member of staff if they receive an offensive message.

5. Making children aware of online safety

- Children will be informed that network and internet use will be monitored.
- Children will be taught about online safety throughout the curriculum and through 'Safer Internet Day' activities and the 4 R's : Respect, Responsibility, Reasoning and Resilience.

- Online safety rules will be posted in appropriate places in school and the children will be reminded of them throughout the year (see Appendix B).
- Through Relationships and Sex Education (RSE) pupils will be taught about online safety and harms. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. There are also other curriculum subjects which include content relevant to teaching pupils how to use the internet safely. For example citizenship education covers media literacy - distinguishing fact from opinion as well as exploring freedom of speech and the role and responsibility of the media in informing and shaping public opinion. It also supports teaching about the concept of democracy, freedom, rights, and responsibilities.
- The schools will help pupils by:
    - helping them to identify who trusted adults are,
    - looking at the different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations such as Childline and Internet Watch Foundation. This should link to wider school policies and processes around reporting of safeguarding and child protection incidents and concerns to school staff (see Keeping Children Safe in Education); and
    - helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported

6. Wellbeing & Online Safety

Elements of online activity can adversely affect a pupil's wellbeing. These include, Self-image and identity, Online reputation, Online bullying, Health, wellbeing and lifestyle. Any pupil can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage and personal circumstance. Some pupils, for example looked after children and those with special educational needs, may be more susceptible to online harm or have less support from family or friends in staying safe online. Support and teaching will be tailored to ensure these pupils receive the information and support they need. Parents and carers will also be offered and provided support via newsletters, information on the website, training sessions and other methods as appropriate. Age specific advice on these potential harms and risks can be found Education for a Connected World framework (appendix A).

7. Names and personal data

- Personal data will be recorded, processed transferred and made available only in accordance with the General Data Protection Regulation.
- Children's full names will not be used anywhere on a school website, blog, app or social media page, unless in exceptional circumstances in which parental permission has been obtained (e.g. to celebrate an individual achievement in a news item).
- Looked After Children or children under Child Protection plans will never have their full name published, within or outside the school.

8. Images of children and their work

We often take photographs and videos of the children. These images of pupils achieving and enjoying activities really do help to promote positive aspects of learning and to share and celebrate children's work at school in an exciting and immediate way.

8.1 Examples of how images may be used within school include:

- As part of a learning activity; e.g. a teacher photographing the children at work and then sharing the pictures in the classroom, allowing them to see their work and make improvements.
- For presentation purposes around the school; e.g. in school wall displays or slideshows that celebrate children's work and achievements.
- As part of a recorded lesson observation; e.g. teachers using a video to help them review and evaluate their practice, and to discuss their lesson with other staff in order to further develop their teaching.

8.2 Examples of how images may be used externally include:

- In the school or Trust prospectus.
- On the school or Trust website.
- In a presentation about the school or Trust and its work, in order to share its good practice with other schools or educators.
- In the media (very rarely); e.g. if a newspaper photographer or television film crew attend an event.

8.3 Our policy regarding publishing images of children and their work:

- To comply with the General Data Protection Regulation, parents and carers are asked for their consent for the school to publish photographs of their child on the website or in publications.
- Images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose.
- Where showcasing examples of pupils work, we only use their first names.
- We do not use a child's name beside a photograph of them.
- Only images of pupils in suitable dress are used.

9. School online content and communications

- Each school's headteacher will take overall responsibility for the school's website, email or text communications, apps, blogs or social media accounts, and will ensure that all content is accurate and appropriate.

10. Acceptable ICT use and online safety for adults

10.1 Staff

- All staff are given a copy of the online safety policy and expected to read it. They are also required to read the Code of Conduct for Safeguarding and Keeping Children Safe in Education Part 1 and Annex A and follow its guidance in relation to online safety.
- Staff are aware they should never 'friend' a child on social networking sites or gaming platforms.
- Staff should not have photos or videos of children on their phone or any other personal device (if they do need to take a photo or video, these should be uploaded onto the school system for school use as soon as possible, and deleted from the personal device)

- Staff should not use school equipment for non-school activities
- Staff must read the 'acceptable ICT use' agreement before using any school ICT resource or equipment
- Staff are made aware that internet use can be monitored and traced to individual users and schools. Discretion and professional conduct is essential.
- If a member of staff discovers or accesses any unsuitable content, or a child tells them about any inappropriate content they have accessed, the member of staff must report this to the school's online safety co-ordinator.
- Staff may use email to contact parents and other outside agencies. These are treated as official means of communication and are only permitted to come from their school email account.
- It is advised that, as much as possible, staff will ensure that their personal devices are connected to the school wifi, in order to ensure suitable blocking, and avoid turning on 3G/4G. Where this is not possible, staff will ensure their devices have a password protection in case of loss or in case children access their devices.

10.2 Parents and carers

- This policy will be made available to parents/carers though the website of each school in the trust and will be mentioned in communications and parent training/ information sessions where appropriate.
- Parents/carers are expected to have due care and awareness of online safety risks that their children may experience at home or in the wider community & take responsibility for managing responsible use by their children.
- Parents/carers are requested to consider the 'acceptable use' guidelines below regarding their use of the internet or online platforms:
    - Take regard of the school's rules regarding children's access to the internet
    - Use appropriate language and forums for expressing views, opinions and requests, so as not to bring the school into disrepute
    - Avoid posting information about pupils or staff
    - Use appropriate channels for complaints (see separate complaints policy)
- Parents are requested to be considerate in terms of language, timing and frequency, when contacting staff by email

10.3 Volunteers and visitors

- All volunteers and visitors providing extra-curricular activities for children are required to read the Code of Conduct for Safeguarding and follow its guidance in relation to online safety.
- Where appropriate, volunteers and visitors will be provided with limited access to the school network.
- The online safety policy will be shared with the Parent Teacher Association (PTA) or equivalent organisation for each school. Our schools expect that any PTA material, e.g. via email communications or social media, is in accordance with the policy.

10.4 Local governors and trustees

- All local governors and trustees are required to read the Code of Conduct for Safeguarding and the online safety policy.
- Local governors and trustees will attend online-safety training as appropriate.

11. Assessing risk

- We review this policy regularly to ensure it is adequate and that its implementation is effective across the curriculum and all aspects of school life.
- New technologies will be examined for educational benefit and a risk assessment will be carried out before use is allowed.
- We assess the risk of children being groomed or at risk of child sexual exploitation. All staff are made aware of risk factors through whole school training.
- We assess the risk of children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology. All staff have completed Prevent training.
- The Trust and its schools will take all reasonable precautions to ensure that users access only appropriate material. However, due to the scale and nature of worldwide internet content, it is not possible to guarantee that unsuitable material will never appear on a computer. The Trust and the schools within it cannot therefore accept liability for material accessed or any consequence of internet access.

12. Handling online safety issues

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Complaints concerning child protection must be dealt with in accordance with the trust's child protection and safeguarding policy.
- Any complaint about staff misuse must be referred to the headteacher.
- Internet browsing history may be looked at in cases where it is deemed necessary.
- Computers, mobile phones or other devices found to contain images or text relating to a safeguarding concern or inappropriate use may be removed from children in situations where parents or police may need access to the information. Devices may be confiscated without the consent of the child. They should be turned off and kept in a sealed envelope.
- Inappropriate images will not be printed or saved. They may be deleted with the child's consent or parents may delete images in the presence of the child.
- Where staff are required to see inappropriate images, messages or other content which has been created/shared/received/stored by a child or another member of staff, a written record will be made of when they were seen, who was present and the reason for viewing them.
- Staff will be offered opportunities for supervision or managers will ensure time for follow up and reflection following experience of distressing situations.
- All actions will be carried out in line with the child protection and safeguarding policy.
- Parents who wish to raise a formal concern or make a complaint should also be referred to the complaints policy.

Appendix A: Useful documents, contacts and links

Child Exploitation and Online Protection (CEOP)
CEOP is a law enforcement agency which aims to help keep children safe from sexual abuse and grooming online. They can provide advice, and anyone can make a report directly to CEOP if something has happened online which has made them feel unsafe, scared or worried.
https://ceop.police.uk/

UK Council for Child Internet Safety (UKCCIS)
A group of more than 200 organisations that work in partnership to help keep children safe online. They have produced a wide range of reviews and guidance documents, including guidance for schools on 'sexting' and guidance for parents/carers whose children are using social media.
https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

NSPCC e-safety resources
Online safety advice and resources for schools and colleges
https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/e-safety-schools/

Keeping safe online: A guide for people with learning disabilities (Care Management Group and CHANGE)
The Care Management Group and CHANGE have produced an easy-read guide to keeping safe online for people with learning disabilities.
http://cmg.co.uk/wp-content/uploads/2017/12/Keeping-Safe-Online-Easy-Read-Guide-Email-Version.pdf

Searching, screening and confiscation, January 2018
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674416/Searching_screening_and_confiscation.pdf

Keeping Children Safe in Education https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

Keeping Children Safe in Education Sept 2019 (draft)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811513/DRAFT_Keeping_children_safe_in_education_2019.pdf

Online Safety. A Practical Guide for Schools (May 2019)
https://www.rm.com/pdf/web/viewer.html?file=~/media/PDFs/Security-and-safeguarding/RM_Esafety_BROCHURE-May19.pdf

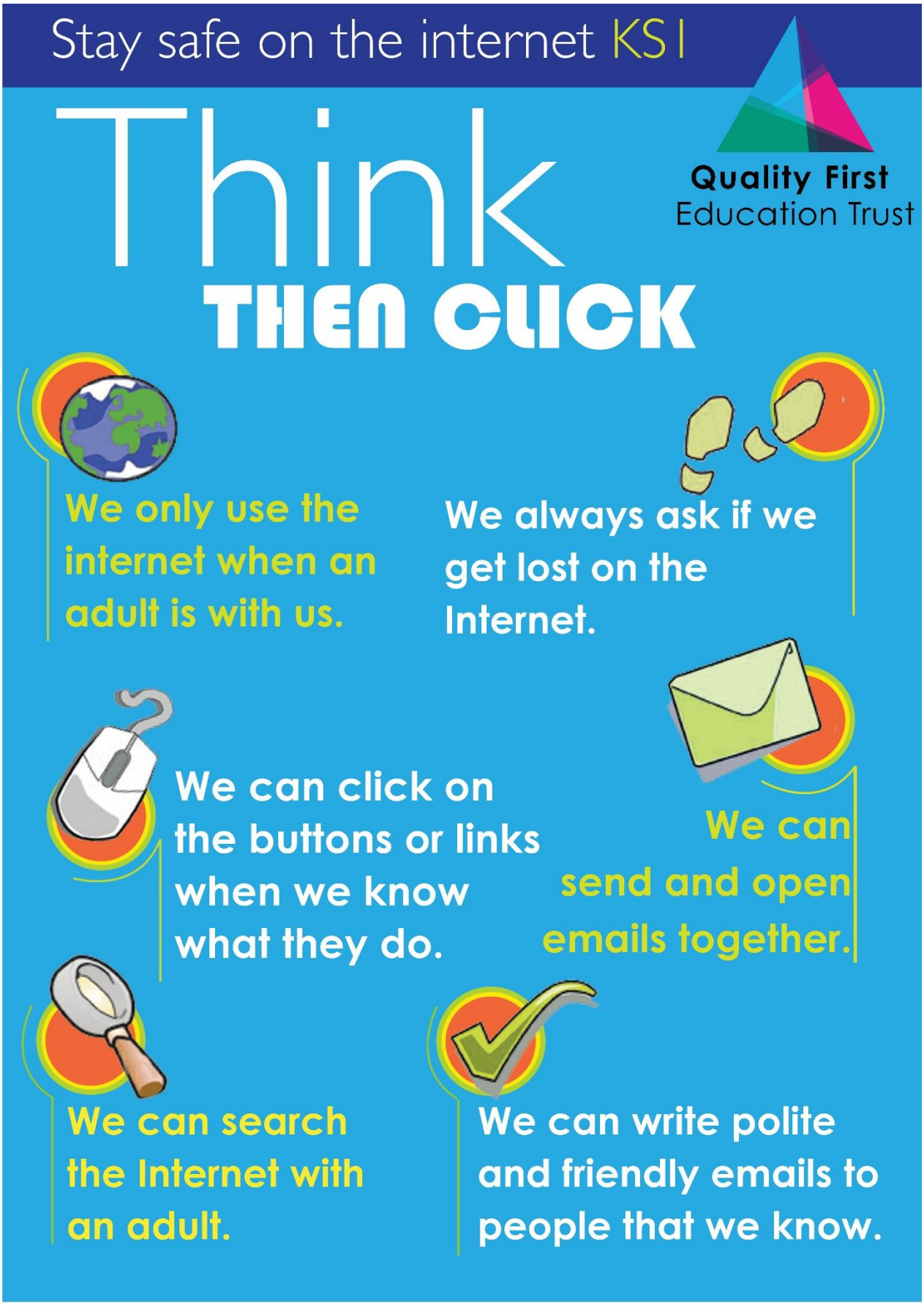
Online Harms White Paper
https://www.gov.uk/government/consultations/online-harms-white-paper

Teaching Online Safety in School (Jan 2019)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf

Education for a Connected World (Feb 2018)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759003/Education_for_a_connected_world_PDF.PDF

Appendix B: Online safety posters for children

Key Stage One:

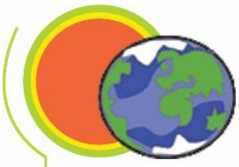


Key Stage Two:

Stay safe on the internet KS2

Think THEN CLICK

Quality First Education Trust



We ask permission before using the Internet.

We only use websites that a member of staff has approved.

We do not use Internet chat rooms.

We immediately turn off the screen or shut a laptop lid if we see any webpage we not sure about and tell an adult.

We tell an adult if we see anything we are uncomfortable with.

We never give out personal information or passwords.

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

We send e-mails that are polite and friendly.

We only e-mail people an adult in school has approved.

We do not open e-mails sent by anyone we don't know.