# Barrowby Church of England Primary School

**E-Safety Policy**

## 1. Introduction

1.1. New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter. Barrowby CE Primary School endeavours to highlight benefits and risks of using technology and provides Safeguarding and education for users to enable them to control their online experience.

## 2. Definition of E-Safety

2.1. Definition of E-Safety Within Lincolnshire, the definition of e-Safety is the proactive and reactive measures to ensure the safety of the child, and adults working with the child, whilst using digital technologies. This extends to policy, training and guidance on the issues, which surround risky behaviours, and encompasses the technical solutions, which provide further safeguarding tools. It should be remembered that digital technology reaches far and wide, not only computers and laptops, but consideration should also be given to technologies such as: iPads, iPod Touches and iPhones; Xbox ; PlayStations; Nintendo Wii and Switch; mobile phones and PDAs, Smart watches and anything else which allows interactive digital communication.

## 3. Aims

3.1. We aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

## 4. The 4 key categories of risk

4.1. Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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** – personal online behaviour that increases the likelihood of, or causes, harm, such as 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; and

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

## 5. Legislation and guidance

5.1. This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
- It also refers to the Department's guidance on protecting children from radicalisation.
- The policy also takes into account the National Curriculum computing programmes of study.
- It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

## 6. Roles and responsibilities

6.1. All governors will:

- The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2).
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

6.2. **The headteacher is responsible for:**

- Ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- Putting in place (with support from ARK) appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly. (with support from ARK)

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

**6.3. The designated safeguarding lead**

- Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well relevant job descriptions.
- The DSL and deputies take lead responsibility for online safety in school, in particular:
- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher, ICT coordinator and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school child protection policy.
- Ensuring that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary

**7. All staff, including contractors and agency staff, and volunteers are responsible for:**

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2) and ensuring that pupils follow the school's terms on acceptable use (appendix 1).
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

**8. Parents are expected to:**

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Parents can seek further guidance on keeping children safe online from the following websites and support the school in promoting e-safety:
    - What are the issues? - UK Safer Internet Centre
    - Hot topics - Childnet International
    - Parent factsheet - Childnet International

- Parents should consult with the school if they have any concerns about their children's use of technology.

## 9. Visitors and members of the community

9.1. Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. They will be provided with a visitor.

## 10. Learning and Teaching

10.1. We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in our school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

10.2. We will provide a curriculum which has E-Safety related lessons embedded throughout. From the National Curriculum computing programmes of study.

10.3. In Key Stage 1, pupils will be taught to:
- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

10.4. Pupils in Key Stage 2 will be taught to:
- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

10.5. The safe use of social media and the internet will also be covered in other subjects where relevant.

10.6. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.
- We will celebrate and promote e-Safety through a planned programme of assemblies and wholeschool activities, including promoting Safer Internet Day each year.
- We will discuss, remind, or raise relevant e-Safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objective for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities through an Acceptable Use Policy which every pupil will sign and be displayed throughout the school.

- School will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button

## 11. Cyber-bullying Definition

11.1. Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

11.2. To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

11.3. The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class.

11.4. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

11.5. All staff receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

11.6. In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

11.7. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so. If staff require it, further advice can be sought from Lincolnshire Safeguarding Children Partnership (LSCP) including Lincolnshire's E-safety officer, Dan Hawbrook (dan.hawbrook@lincolnshire.gov.uk)

## 12. Examining electronic devices

12.1. School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

12.2. If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police.

12.3. Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

## 13. Staff Training (CPD)

13.1. As part of the induction process all new staff members will receive information and guidance on the E-Safety Policy, e-security, reporting procedures and read and sign the school's Acceptable Use Policy.

13.2. All staff members will receive regular information and training on e-Safety issues, as well as updates as and when new issues arise. (for example through emails, e-bulletins and staff meetings).

13.3. All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.

13.4. The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

13.5. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

13.6. Volunteers will receive appropriate training and updates, if applicable.

13.7. More information about safeguarding training is set out in our child protection and safeguarding policy.

## 14. Managing ICT Systems and Access

14.1. The school will agree on which users should and should not have internet access and the appropriate level of access and supervision they should receive.

14.2. All users will sign an Acceptable Use Policy (AUP) provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT system and that such activity will be monitored and checked.

14.3. All internet access will be undertaken alongside a member of staff or, if working independently, a member of staff will supervise at all times.

14.4. Members of staff will access the internet using their log in and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their ID or password. They will abide by the school AUP at all times.

## 15. Managing Filtering

15.1. To provide assistance in safeguarding we use Internet filtering. The school has the Netsweeper Internet filtering system in place which is managed by the school and ARK. Banned phrases and websites are identified and blocked.

15.2. The school has a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training/online safety lesson.

15.3. If staff or pupils discover an unsuitable site, it must be reported to the headteacher immediately.

15.4. If users discover a website with potentially illegal content, this should be reported immediately to the headteacher. The school will report such incidents to appropriate agencies including Internet Service Provider (ISP), Police, CEOP or the Internet Watch Foundation (IWF).

15.5. Any amendments to the school filtering policy or block and allow lists will be checked and assessed by the headteacher prior to being released or blocked.

15.6. The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

## 16. E-Mail

16.1. Staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.

16.2. Staff should not send personal emails to pupils.

## 17. Social Networking

17.1. Staff will not post content or participate in any conversations which will be detrimental to the image of the school. Staff who hold an account should not have parents or pupils as their 'friends'. Doing so could result in disciplinary action or dismissal.

17.2. School blogs or social media sites should be password protected and run from the school website with approval from the Senior Leadership Team.

## 18. Pupils Publishing Content Online

18.1. Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.

18.2. Pupils' full names will not be used anywhere on the website, particularly in association with photographs and video.

18.3. Permission is obtained from the parents/carers before photographs and videos are published.

18.4. Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment.

18.5. Pupils and staff are not permitted to use their own portable devices to store images/video/sound clips of pupils.

## 19. Pupils' use of personal devices

19.1. Pupils by permission of the Headteacher can bring mobile phones/devices/smart watches onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into the school office before the start of the school day and collected at the end of the day.

19.2. Pupils who do not follow the school policy relating to the use of mobile phones will not be permitted to bring their mobile phones into school.

## 20. Staff or parent use of personal devices

20.1. Staff are not permitted to use their own mobile phones or devices for contacting children or their families within or outside of the setting in a professional capacity. Staff should always use school phone to contact parents. (unless in an emergency or approved by the Head Teacher)

20.2. Staff or volunteers will not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school provided equipment for this purpose.

20.3. If a member of staff breaches the school policy then disciplinary action may be taken.

20.4. Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode, Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods, whilst pupils are present, unless permission has been granted.

20.5. At school events parents/carers are permitted to take pictures of their child in accordance with school protocols. However, such photographs including other parents' children should not be shared on social networking sites.

## 21. Staff using work devices outside school

21.1. All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date – always install the latest updates
- Work devices must be used solely for work activities
- If staff have any concerns over the security of their device, they must seek advice from SLT

## 22. General Data Protection (GDPR) and e-Safety

22.1. Data must always be processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected. GDPR is relevant to e-safety since it impacts on the way in which personal information should be secured on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.

22.2. Staff need to ensure that care is taken to ensure the safety and security of personal data regarding all of the school population and external stakeholders, particularly, but not exclusively: pupils, parents, staff and external agencies. Personal and sensitive information should only be sent by e mail when on a secure network. Personal data should only be stored on secure devices.

22.3. In the event of a data breach, the school will notify the School's Data Protection Officer (DPO) immediately, who may need to inform the Information Commissioner's Office (ICO).

## 23. Support for Parents

23.1. Parents' attention will be drawn to the school's e-Safety policy and safety advice in newsletters, the school website and e-Safety information workshops.

23.2. The school website will be used to provide parents with timely and meaningful information about their children's school lives and work to support the raising of achievement. The website will also provide links to appropriate online-safety websites.

## 24. Assessing Risks

24.1. The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

## 25. Equality of Educational Opportunity

25.1. The school has regard to the Code of Practice for children with Special Educational Needs and disability (SEND) and strives to ensure those children's special needs are identified and met, with the support of outside agencies and the use of individual instruction on e-safety where appropriate. The school will take into consideration the effect of any SEND and will put in place strategies to support children with disabilities. We will ensure that we do not discriminate against children or other members of the school community on grounds of gender, age, religious, cultural or ethnic differences, all of which have implications for equality of educational opportunity. For children with Autistic Spectrum Disorders – both diagnosed and those under diagnosis/assessment – the school will make reasonable adjustment and adaptations without compromising the health, safety and well-being of the other children. The school are guided by the Autism Education Trust (AET) set of National Standards which describe the key factors common to good practice for pupils with autism.

## 26. Introducing the e-Safety policy to pupils

26.1. E-Safety throughout our curriculum with a rigorous knowledge progression in place. This includes learning about topics such as; online bullying, the importance of passwords and how to stay safe on social media. In school, we also discuss topics such as fake news and advertising, so children are well informed to make safe decisions.

26.2. Children need to know how to keep themselves safe, as well as how to react if they encounter unsafe content or feel uncomfortable online. We always emphasise the importance of keeping adults informed of their activities online. As well as focusing on Online Safety across our curriculum, we invite experts into school to deliver E-Safety workshops, further developing our children's understanding of how to stay safe online. We work alongside the Lincolnshire Stay Safe Partnership to deliver these.

## 27. Useful websites:

- CEOP is a part of the UK police force dedicated to the eradication of child sexual abuse. www.ceop.gov.uk

- IWF (Internet Watch Foundation) provides the UK hotline to report criminal online content. www.iwf.org.uk
- Digital citizenship is about building safe spaces and communities, understanding how to manage personal information, and about being internet savvy - using your online presence to grow and shape your world in a safe, creative way, and inspiring others to do the same. www.digizen.org

**28. E-Safety Policy Review**

This policy is reviewed by the Head teacher, staff and Governors in accordance with Barrowby This policy is reviewed by the Head teacher, staff and Governors in accordance with Barrowby School's Policy and Review Cycle for approval by the Full Governing Body, every 3 years.

Last reviewed: November 2023
Next review: November 2026

*Barrowby Church of England Primary School*

**Pupil's Acceptable Use of Computers Policy**

I understand that using the computer network is a privilege which can be removed from me. When using the computer, I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
  - I click on a website by mistake
  - I receive messages from people I don't know
  - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- I will be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**

If I break any of these rules, I will report it to my teacher as soon as possible and realise that I may be in trouble, but my honesty will be recognised.

Please complete and return the proforma below;

✂ _____

**Internet Permission Form**

As a school user of the Internet, I agree to comply with the school rules on its use. I will use the network in a responsible way and observe all the restrictions explained to me by the school.

Pupil's signature: _____ Date:

Parent's/Carer's Declaration As the parent or carer of the pupil signing above, I grant permission for my son or daughter to use electronic resources and the Internet.

I understand that pupils will be held accountable for their own actions. I also understand that some material on the Internet may be objectionable and I accept responsibility for setting standards for my son or daughter to follow when selecting, sharing and exploring information and media.

Parent's/Carer's signature: _____ Date:

Pupil's Name: _____ Class:

*Barrowby Church of England Primary School*

**School Acceptable Use Policy**

Staff, Governor and ICT Code of Conduct ICT and the related technologies such as email, the internet and mobile devices are an expected part of our working life in school. This policy is designed to ensure all staff are aware of their professional responsibilities when using any form on ICT.

- All staff and governors are expected to sign this policy and adhere at all times to its contents.
- I appreciate that ICT includes a wide range of systems and devices including mobile phones, PDAs, digital cameras, email, social networking and may include personal ICT devices when used for school business.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activities carried out under my user name.
- I will only use the school email, internet and any other related technologies for professional purposes.
- I will ensure that personal data is kept secure and used appropriately, whether in school, taken out of school or used remotely when authorised by the headteacher or governing body.
- I will not install any hardware or software without permission.
- I will respect copyright and intellectual property rights.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with consent of the parent, carer or staff member. Images will not be distributed outside the school network without permission.
- I will ensure that my online activity both in school and outside will not bring my professional role into dispute and know that my Internet and email use may be subject to monitoring.
- I will support the school's e-safety policy and help pupils to be safe.
- I will report any incidents of concern regarding children's safety to the designated safeguarding lead or the headteacher.
- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serious infringements may be referred to the police.

**User Signature:**

I agree to follow the code of conduct and support the safe use of ICT throughout the school;

Full Name _____

Job Title _____

Signature _____ Date _____