Belonging, Believing; Together Succeeding.

Policy: E-Safety Policy

Date Reviewed by Staff:	June 2019
Date Reviewed by Education Committee:	July 2019
Date Ratified by Full Governing Body:	July 2019
Next Review Date: (3 years unless otherwise advised)	June 2022

Barrington C of E Primary School
E-Safety Policy

Our Vision

Our vision as a Church of England primary school, deeply rooted in a strong Christian tradition, is to develop happy, young people with enquiring minds, a lifelong love of learning, respect for themselves, others and the environment so that they will have the skills, resilience and adaptability to thrive in a rapidly changing world.

The school's policy is that no adult or child is allowed to use school computers without having signed an **acceptable user statement.** Visiting pre-school pupils will be covered by the responsible adult accompanying them having signed a statement on

E-Safety in schools is a child safety and not an ICT issue. Therefore this policy should be viewed alongside other Safeguarding policies including those for behaviour, anti-bullying, personal, social and health education (PSHE) and for citizenship

Contents

- The background to this policy
- Rationale
- Teaching and Learning Using Online Technologies
- Technology in School
- The E-Safety Curriculum
- Safeguarding Children Online
- Responding to Incidents

Background to the policy

The purpose of this policy is to describe the safeguarding measures in place for adults and children in school:

- the ground rules we have developed in school for using the Internet and online technologies
- how these fit into the wider context of our other school policies
- the methods used to protect children from sites containing pornography, racist or politically extreme views and violence.

Ultimately, the responsibility for setting and conveying the standards that children are expected to follow when using technology, media and information resources, is one the school shares with parents and carers. At *Barrington C of E Primary School*, we feel that the most successful approach lies in a combination of site filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

The development of our safety policy involved…

- Headteacher
- E-Safety Co-ordinator
- Senior lead teacher
- Governor

- Governor
- TA

It was presented to the governing body and ratified on July 2019
It will be available on the school website.

Rationale

At Barrington C of E Primary School, we believe that the use of information and communication technologies in schools brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively.
The use of these exciting and innovative technology tools in school and at home has been shown to raise educational standards and promote pupil achievement. Yet at the same time we recognise that the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:
• Access to illegal, harmful or inappropriate images or other content
• Unauthorised access to / loss of / sharing of personal information
• The risk of being subject to grooming by those with whom they make contact on the internet.
• The sharing / distribution of personal images without an individual's consent or knowledge
• Inappropriate communication / contact with others, including strangers
• Cyber-bullying
• Access to unsuitable video / internet games
• An inability to evaluate the quality, accuracy and relevance of information on the internet
• Plagiarism and copyright infringement
• Illegal downloading of music or video files
• The potential for excessive use which may impact on the social and emotional development and learning of the young person.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. E-Safety issues can also affect adults who work or are associated with the school. For example school and personal data being entered on web/social networking sites, fraudulent email traps and cyberbullying. It is impossible to eliminate risk completely. It is therefore essential, through good educational provision to manage the risk and deal with any threat to safety.

Teaching and Learning Using Online Technologies

The internet is a part of everyday life for education, business and social interaction.
Benefits of using online technologies in education include:

- Access to world-wide educational resources
- Inclusion in the National Education Network (NEN) connecting all UK schools and resources
- Access to experts who would otherwise be unavailable
- Access to anytime, anywhere learning
- Collaboration across schools, networks of schools and services

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. At Barrington C of E Primary School we believe that a comprehensive programme of E-Safety education is vital for developing our pupils' ability to use technologies safely. This is achieved using a combination of discrete and embedded activities drawn from a selection of appropriate materials (see cross references) and external training providers. We believe that just as children learn how to swim by going to a swimming pool so they will learn safe life-long online behaviours by accessing and using the internet. Members of staff constantly monitor pupils' use of the internet and other technologies and publishing tools. Our programme for E-Safety education is evidenced in teachers' planning either as discrete or embedded activities.

The use of the internet in the curriculum needs careful planning, and it should not be assumed that the children have the skills and knowledge of how to work safely in an online environment – for example how to use search engines safely. Therefore, if the internet is to be used, the teacher should ensure that these points are covered in the interest of accessibility and also of safety. They will also be responsible for ensuring pupils use the correct log on. The teaching of specific ICT skills is currently allocated time, together with a slot in the ICT suite and also with the use of ipads and chrome books within the classroom. It may involve the teacher working with the whole class or with a group, teaching them specific skills. Messages involving Risks and Rules and Responsibilities are taught and/or reinforced as detailed in the school's Acceptable Use Policies (see cross references).

Technology

The school's ICT infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by both the East of England Broadband Network (E2BN) and the Local Authority's Education ICT Service.

E2BN's Protex web filtering system received full Becta (British Educational Communications and Technology Agency) accreditation in 2007 by blocking over 90% of all inappropriate material. E2BN also manage a distributed caching service which is integrated with the web filtering service. ????

Ref: E2BN Website

This helps to ensure that staff and pupils rarely encounter material which is inappropriate or offensive. If / when they do, the school's AUPs and E-Safety education programme ensure that they are equipped to deal with any issues in the most appropriate way.

Technologies regularly used by pupils and adult stakeholders include (but not exclusively):

Staff:

- Smartboards, Laptops, desktops, ipads and chrome books
- Cameras and video cameras, visualisers
- Internet, E-mail, central hosting including access to SIMS and confidential pupil information

Pupils:

- Ipads, chrome books and desktops
- Cameras and video cameras, visualisers
- Internet, school website, discussion forums, blogs and other communication tools
- Other peripherals such as programmable toys, dataloggers, control technology equipment

Others on school premises:

- Limited access to school systems such as filtered internet access using a visitor login.

Whilst we recognise the benefits of individual pupil logins to our school network, in our school we prefer to use year group logins for ease of access. All members of staff have individual, password protected logins to the school network and visitors to the school can access part of the network using a generic visitor login and password. The school's network can either be accessed using a wired or wireless connection. However, the wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the school office. School staff and pupils are **not** permitted to connect personal devices to the school's wireless network and the wireless key is **not** given to visitors to the school.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Pupil's mobile phones will not be brought to school without prior permission from the Headteacher. They will not be used during lessons or formal school time and will be held securely with a member of staff. The sending of abusive or inappropriate text messages is forbidden.

The E-Safety Curriculum

In line with recommendations in the E-Safety briefing for Ofsted Inspectors (Sept 2017???) we have planned a range of age-related teaching and learning opportunities to help our pupils to become safe and responsible users of new technologies. These opportunities may include:

- Termly Key stage assemblies
- Specific activities during safety day (traditionally held in February) and Anti-bullying week (held traditionally in November)
- Age-related classroom activities using the ThinkUKnow materials
- ACE accredited scheme for pupils
- Related work in PSHE lessons
- Posters and reminders in and around the school

Safeguarding Children Online

At Barrington C of E Primary School, we recognise that different users will be expected to use the school's technology systems in different ways – appropriate to their age or role in school. We acknowledge the need to:

Equip children to deal with exposure to harmful and inappropriate content and contact, and equip parents to help their children deal with these things and parent effectively around incidences of harmful and inappropriate conduct by their children.

UKCCIS (The UK Council for Child Internet Safety) – June 2008

The school has published Acceptable Use Policies for pupils and staff who sign to indicate their acceptance of our AUPs and relevant sanctions which will be applied should rules be broken. Please see cross references for full details.
Any known or suspicious online misuse or problem will be reported to the designated E-Safety Co-ordinator for investigation/ action/ sanctions.

All staff should have an awareness of the Prevent Duty and their responsibilities with regard to this. The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place. Schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. As with other online risks of harm, every teacher needs to be aware of the risks posed by the online activity of extremist and terrorist groups. Internet safety will usually be integral to a school's ICT curriculum and can also be embedded in PSHE and SRE.

Responding to Incidents – *(Education Child Protection Service – June 2010?? Still correct date?)*

It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an E-Safety incident occurs or they suspect a child is at risk through their use of technology. It is important that responses to E-Safety incidents are consistent with responses to other incidents in school. This may mean that serious actions have to be taken in some circumstances.
If an E-Safety incident occurs we will follow the agreed procedures for dealing with incidents including internal sanctions and involvement of parents (for ICT, this may include the deactivation of accounts or restricted access to systems as per the school's AUPs – see appendix). Where the school suspects that an incident may constitute a Child Protection issue, the usual Child Protection procedures will be followed.

Dealing with Incidents and Seeking Help

If a concern is raised, refer immediately to the designated person for child protection. If that is not possible refer to the headteacher or, if necessary, the Chair of Governors.
It is their responsibility to:

Step 1: Identify who is involved – any combination of child victim, child instigator, staff victim, or staff instigator
Step 2: Establish the kind of activity involved and whether it is illegal or inappropriate. If in doubt they should consult the Education Child Protection Service helpline.
Step 3: Ensure that the incident is documented using the standard child protection incident logging form (see appendix)
Depending on the judgements made at steps 1 and 2 the following actions should be taken:
Staff instigator – follow the standard procedures for Managing Allegations against a member of staff. If unsure seek advice from the Local Authority Designated Officer or Education Officer.
Staff victim – Seek advice from your Human Resources (HR) provider and/or Educational Child Protection Service
Illegal activity involving a child – refer directly to Cambridgeshire Constabulary – 0845 456 4564 – make clear that it is a child protection issue
Inappropriate activity involving a child – follow standard child protection procedures. If unsure seek advice from Education Child Protection Service helpline.
Equally, if the incident involves or leads to an allegation against a member of staff, the school will follow the agreed procedures for dealing with any allegation against a member of staff (see appendix).

Terms used in this policy

AUP: Acceptable Use Policy.
A document detailing the way in which new or emerging technologies may/may not be used – may also list sanctions for misuse.

Child: Where we use the term 'child' (or its derivatives), we mean 'child or young person'; that is anyone who has not yet reached their eighteenth birthday.

E-Safety: We use E-Safety, and related terms such as 'online', 'communication technologies', and 'digital technologies' to refer to all fixed and mobile technologies that children may encounter, now and in the future, which might pose E-Safety risks. We try to avoid using the term 'ICT' when talking about E-Safety as this implies that it is a technical issue – which is not the case. The primary focus of E-Safety is child protection: the issues should never be passed solely to technical staff to address.

PIES: A model for limiting E-Safety risks based on a combined approach to **P**olicies, **I**nfrastructure and **E**ducation, underpinned by **S**tandards and inspection. Whilst not explicitly mentioned in this policy, this model provides the basis for the school's approach to E-Safety.

Safeguarding: Safeguarding is defined (for the purposes of this document) as the process of increasing resilience to risks when using technology through a combined approach to policies and procedures, infrastructure and education, underpinned by standards and inspection. E-Safety is just one aspect of a much wider safeguarding agenda within the UK, under the banner of *Every Child Matters: Change for Children*. Those with responsibility for the development and delivery of E-Safety policies should embed their work within the wider safeguarding agenda, and work across services to ensure that they are delivering the best possible opportunities for the children and young people in their care.

Schools: For ease of reading we refer predominantly to schools within this publication, but the underlying principles can be applied equally to any setting with responsibility for educating or safeguarding children and young people.

Users: We use this term, and related terms such as service users and end users, to mean those people who will ultimately be bound by the provisions of an AUP. This might be pupils, staff, parents and carers, or members of the wider community, depending on provisions of your AUP or the context in which you operate.

Cross references:

- Professional boundaries in relation to your personal internet use and social networking online – advice to staff (LSCB)

- Behaviour policy
- Safeguarding and Child Protection
- SRE (Sex and Relationships Education)
- Citizenship and PSHE
- Safer Working Practices
- Data Protection Policy
- County guidance (e.g. Use of Digital Images, e-mail)
- AUPs- staff, pupil, parents
- Anti-Bullying Policy
- School Complaints Procedure
- LA Infrastructure guidance (E2BN)
- Cambridgeshire Progression in ICT Capability Materials
- Risk assessment log/Incident Log-located in CP file (held in Headteacher's office)

- ICT Policy