Brimpton Church of England
Primary School

E-SAFETY POLICY

Brimpton C of E Primary School

Approval Date: June 2022
Next Review Date: September 2025

Brimpton Primary School
Brimpton Lane
Reading
RG7 4TL

E-Safety Policy

Brimpton Church Of England Primary School

Document Control

Version:	V1	Date Created	June 2022
Author:	HD/SV	Date Modified	
Status:	***Statuory***	Frequency of Review	Every 3 Years

Head Teacher	Sign & Date:	
Chair of Governing Body	Sign & Date:	

Date Approved:	January 2025		
Next Review Date:	Jan 2028	Date Reviewed:	
Next Review Date:	Jan 2031	Date Reviewed:	
Next Review Date:	Jan 2034	Date Reviewed:	

1. Introduction

This policy sets out Brimpton Primary School's requirements and expectations on the use of the internet and related communication technologies. That they be used appropriately and safely.

The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Headteacher and Governors to the Senior Leaders and Classroom Teachers, support staff, parents, and pupils themselves.

This e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying, child protection, safe use of images and social networking).

2. Purpose

This policy aims to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

3. Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors,) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

4. Roles and Responsibilities

4.1. Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors on receiving information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor.

4.2. **Headteacher**

- is responsible for ensuring the safety (including e-safety) of members of the school community
- is responsible for ensuring that relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff
- is responsible for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- is responsible for ensuring that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- is responsible for monitoring the school's social media presence (closed Facebook page and group)

4.3. **Teaching and Support Staff**

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Responsible Internet Use Statement
- they report any suspected misuse or problem to the Headteacher for investigation
- digital communications with pupils (email / Virtual Learning Environment) is on a professional level
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety policy and student responsible internet use statement
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and handheld devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

4.4. **Pupils:**

Will be expected to have a good understanding :

- of their responsibilities when using the school ICT systems in accordance with the Student /Responsible Internet Use statement, sent out annually, which they will be expected to sign before being given access to school systems. (At KS1 it would be expected that parents / carers would sign on behalf of the pupils)
- of research skills and the need to avoid plagiarism and uphold copyright regulations
- of the need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- of the school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- of the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

4.5. **Parents / Carers**

The school will take every opportunity to help parents understand these issues through parents' evenings or newsletter or website.

Parents and carers will be responsible for:

- endorsing (by signature) the Student Responsible Internet Use statement

5. Policy Statements

5.1. **Education /Training**

Pupils

The education of pupils in e-safety is an essential part of the school's e-safety provision. E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- pupils will be taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- pupils will be taught to acknowledge the source of information used and to respect copyright

Parents/carers

The school will provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- http://www.childnet-int.org/
- http://www.getnetwise.org/
- http://www.safekids.com/

Staff
All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and student responsible internet use statement

Governors
Governors will take part in e-safety training / awareness sessions, with particular importance for those members involved in ICT / e-safety / health and safety / child protection.

5.2. Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed under the guidance of our Local Authority Technical Support team
- WAN email & web services are managed in conjunction with Elmdale IT.
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems.
- All users will be provided with a username and password by their teacher who will keep an up to date record of users and their usernames.
- The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and is kept in a locked drawer
- The headteacher and internet safety link governor will have admin rights on both the Facebook page and group.
- The Facebook page will be reviewed monthly and all old posts will be deleted so that to ensure relevant information is conveyed to current academic year groups. Only one years worth of information will be kept active.

5.3. Use of digital and video images - Photographic, Video

5.4. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Please refer to the Data Protection Policy.
(This policy is due for review pending the new Data Protection Bill coming into force May 2018).

5.5. **Communications**

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff, Governors and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff, governors and pupils or parents / carers (email, chat, school social media etc.) must be professional in tone and content.

6. Breaches of the Policy

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures and reported to the governors by the Head teacher.

7. Review

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.