“I have come in order that you might have life – life in all its fullness.”
John 10:10

e-Safety Policy

Policy reviewed:	22/2/2017
Next review:	Spring 2020
Signed (Headteacher):	R. Kaye
Statutory policy: Yes/No **On school website:** Yes/No	

E-SAFTY POLICY

1. Introduction

This policy sets out the ways in which the school will:

- educate all members of the school community on their rights and responsibilities regarding the use of technology;
- build both an infrastructure and culture of e-Safety;
- work to empower the school community to use the Internet as an essential tool for lifelong learning.

This policy is used in conjunction with other school policies, including:

- Child Protection and Safeguarding Policy
- ICT Acceptable Use Policy (AUP)
- Social Media and Social Networking Policy

2. Scope of policy

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

The Education and Inspections Act 2006 empowers Headteachers, 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 such as cyberbullying, which may take place out of school, but are linked to membership of the school.

The school will manage e-Safety as described within this policy and associated behaviour and anti-bullying policies, and will inform parents and carers of known incidents of inappropriate e-Safety behaviour that take place in and out of school.

3. Schedule for development, monitoring and review

The implementation of the e-Safety policy will be monitored by the e-Safety Working Group led by the Computing and ICT Subject Leader. The working group will look at:

- the log of reported incidents;
- surveys or questionnaires completed by learners, staff, parents and carers;
- assessment of children against the e-Safety curriculum.

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

4. Roles and responsibilities

Role	Responsibility
Governors	• Our e-Safety Link Governor is Neil Douthwaite • e-Safety Governor works with the Headteacher and Computing and ICT Subject Leader to: (a) monitor, evaluate and report back to the Governing Body; (b) review the effectiveness of the e-Safety Policy.

Headteacher/ Designated Safeguarding Lead	• Create a culture where staff and learners feel able to report incidents • Ensure that there is a system in place for monitoring e-Safety • Follow correct procedure in the event of a serious e-Safety allegation being made against a member of staff or pupil • Ensure that the school infrastructure/network is as safe and secure as possible • Ensure that policies and procedures approved within this policy are implemented • Log, manage and inform others of e-Safety incidents • Ensure all staff are aware of the procedures outlined in policies relating to e-Safety • Work with School Council to ensure all children understand the importance of e-Safety
Computing and ICT Subject Leader	• Lead the e-Safety Working Group • Ensure that all staff receive suitable CPD to carry out their e-Safety roles • With the Headteacher, monitor and evaluate ICT activity in lessons, extracurricular and extended school activities
Technical Support Provider	• Ensure the school's ICT infrastructure is as secure as possible • Maintain and inform the Headteacher of issues relating to filtering • Keep up to date with e-Safety technical information and update others as relevant • Ensure use of the network is regularly monitored in order that any misuse can be reported to the Headteacher for investigation • Ensure monitoring systems are implemented and updated • Ensure all security updates are applied (including anti-virus and Windows)
Teachers and LSAs	• Participate in any training and awareness-raising sessions • Read, understand and sign the Staff AUP • Act in accordance with the AUP and e-Safety Policy • Report any suspected misuse or problems to the Headteacher • Monitor ICT activity in lessons, extracurricular and extended school activities
Pupils	• Understand and agree with the Pupil AUP • Participate in e-Safety activities, follow the AUP and report any suspected misuse • Understand that the e-Safety Policy covers actions out of school that are related to their membership of the school
Parents and Carers	• Endorse (by signature) the Pupil AUP • Discuss e-Safety issues with their child(ren) and monitor their home use of ICT systems (including mobile phones and games devices) and the Internet • Keep up to date with issues through newsletters and other opportunities • Inform the Headteacher of any e-Safety issues that relate to the school

5. Technical infrastructure

The school ensures, when working with our technical support provider that the following guidelines are adhered to:

- The School ICT systems are managed in ways that ensure that the school meets e-Safety technical requirements.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Access to the school network and Internet will be controlled.
- The Internet feed will be filtered and monitored.

6. Data protection

The school will:

- at all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse;
- use personal data only on secure password-protected computers;
- ensure that users are properly "logged-off" at the end of any session in which they are accessing personal data;
- safely store or transfer data (such as end-of-year reports) using Somerset Learning Platform (SLP) or secure password-protected devices;
- make sure data is deleted from the device or SLP once it has been transferred or its use is complete.

7. Use of digital and video images

Photographs and video taken within school are used to support learning experiences across the curriculum, to share learning with parents/carers on our school's learning platform and to provide information about the school on the website. The school will undertake the following:

- When using digital images, instruct staff to educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.
- Allow staff to take images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.
- Make sure that pupils' full names will not be used anywhere on the school website, particularly in association with photographs.
- Parents/carers are asked for parental consent for their child's image and their work to be used on the website and around the school.
- Parents/carers who do not give permission are asked to put this in writing to the school. The Online Safeguarding lead receives these letters and makes class teachers aware.
- Obtain written permission from parents or carers before images or videos of pupils are electronically published.
- Keep the written consent where pupils' images are used for publicity purposes, until the image is no longer in use.

8. Communication

A wide range of communications technologies have the potential to enhance learning. The school will:

- **with respect to email via DB Primary**
  (a) ensure that any digital communication between staff and pupils is professional in tone and content;
  (b) make users aware that email communications are monitored by the Computing and ICT Subject Leader, who will report to the school Headteacher/ Designated Safeguarding Lead if the content is unsuitable.
- **with respect to mobile phones**
  (a) allow staff to bring mobile phones into school but must only use them during lunchtimes unless they have the permission of the Headteacher;
  (b) advise staff not to use their personal mobile phone to contact pupils, parents and carers;
  (c) provide a school mobile phone for activities that require them.

9. World Wide Web

- If pupils discover unsuitable sites they must activate the Hector safety button and report it to an adult immediately
- School will ensure that the use of Internet-derived materials by pupils and staff complies with copyright law.

10. Social media

All staff at Christ Church C of E First School understand they cannot add or be friends with pupils or ex-pupils on social media sites such as Facebook or Instagram. Staff should have their settings on such sites as “Private” so pupils/ex-pupils cannot access their accounts. Staff should be aware at all times of maintaining professional conduct on social media sites.

11. YouTube

YouTube will only be used as a teaching tool at Christ Church.

Children will not have access to YouTube and if seen accessing YouTube, a member of staff will ask the pupil to close the page. YouTube at no time should be accessed in front of pupils, and the teacher teaching that lesson must watch all materials shown to pupils prior to the lesson. All links to the videos shown must be on plans prior to teaching the lesson.

12. Reporting and response to incidents

- Complaints of Internet misuse will be reported to the Headteacher.
- The Headteacher will investigate the incident and log the incident in the Computing and ICT Subject Leader’s file.
- Parents will be informed of the incident where necessary.
- The Headteacher and the Computing and ICT Subject Leader will reflect on the incident and consider changes in practice.