All Saints' Church of England Primary School

WHOLE SCHOOL E-SAFETY POLICY

"Loving to Learn, learning to Love"

"A new command I give you, Love one another.

As I have loved you, so you must love one another."

John 13:34

Ratified by Full Board of Governors: 09.11.2021 Review date: Autumn 2022

Policy Contents

1. INTRODUCTION

All Saints' Primary School is committed to e-safety and fully acknowledges its part in the Safeguarding and Behaviour and Anti-bullying Policies and procedures of our school. It is expected that every member of All Saints' Primary School, which includes parents and carers, will act at all times in a responsible, safe and professional way.

We believe there are great benefits and opportunities given by the internet. With new technologies fast becoming integral to children's lives today, both within school and out in the community, it is imperative that the school embraces their use.

This guidance identifies the risks and the steps we take to avoid them, showing that All Saints' CE Primary School is committed to promoting a safe and responsible attitude. We aim to minimise the risk while continuing to benefit from the education opportunities the new technologies present.

2. AIMS AND OBJECTIVES

E-Safety encompasses the use of new technologies, Internet and electronic communications such as mobile phones, 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.

The e-Safety Policy has been written by the school's IT Manager. It will be reviewed at least annually, with changes made immediately if technological or other developments so require.

The school's e-Safety policy will operate in conjunction with other policies including those for Behaviour, Anti-Bullying, Curriculum and Safeguarding.

Many of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the Internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites, pictures online or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour. It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

3. E-SAFETY CO-ORDINATOR

The E-safety co-ordinator is responsible for the awareness and commitment for e-safety throughout the school maintaining e-safety guidance, Acceptable use policies and any other relevant documentation, reviewing when appropriate and making relevant changes.

Your E-Safety Co-ordinators are Mr D Roberts (Acting Head), Mrs A Forster (Assistant Head), Mr J Smithson (IT Manager)

4. ROLES AND RESPONSIBILITIES

E-Safety is recognised as an essential aspect of strategic leadership in our school and the Headteacher, with the support of governors, aims to embed safe practices into the culture of the school. Our school's e-Safety Coordinator is the Assistant Head teacher who will report to the Head teacher before taking any action.

Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance through liaison with the Safeguarding Officer from the local governing body and through organisations such as The Child Exploitation and Online Protection (CEOP) organisation. The school's e-Safety Coordinator ensures that the Headteacher, senior management team and governors are updated as necessary.

Governors need to have an overall understanding of e-Safety issues and strategies to minimise risks. We ensure our governors are aware of our local and national guidance on e-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

The following table details each group's various roles and responsibilities:

Role	Key Responsibilities
Headteacher/Deputy Head Teachers	• To take overall responsibility for e-Safety provision • To take overall responsibility for data and data security • To ensure the school uses an approved, filtered Internet service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their e-Safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious E-Safety incident. • To receive regular monitoring reports from the E-Safety Co-ordinator

	• To ensure that there is a system in place to monitor and support staff who carry out internal e-Safety procedures (e.g. IT technician)
ICT Co-ordinator/E-Safety Co-ordinator	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-Safety policies / documents • Promotes an awareness and commitment to e-safeguarding throughout the school community • Ensures that e-Safety education is embedded across the curriculum • Liaises with school ICT technical staff • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident • To ensure that an e-Safety incident log is kept up to date • Facilitates training and advice for all staff • Is regularly updated in e-Safety issues and legislation, and aware of the potential for serious child protection issues to arise from: - Sharing of personal data - Access to illegal / inappropriate materials - Inappropriate on-line contact with adults / strangers - Potential or actual incidents of grooming - Cyber-bullying and use of social media - To oversee the delivery of the e-Safety element of the Computing curriculum
Governors	• To ensure that the school follows all current e-Safety advice to keep the children and staff safe • To approve the e-Safety Policy and review the effectiveness of the policy. • To support the school in encouraging parents and the wider community to become engaged in e-Safety activities
Network Manager/IT Technician	• To report any e-Safety related issues that arises, to the e-Safety coordinator • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • The school's policy on web filtering is applied and updated on a regular basis • That he / she keeps up to date with the school's E-Safety policy and technical information in

	order to effectively carry out their e-Safety role and to inform and update others as relevant • That the use of the network remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the e-Safety Co-ordinator / Headteacher for investigation / action / sanction • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster • To keep up-to-date documentation of the school's e-security and technical procedures
Teachers	• To embed e-Safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All Staff	• To read, understand and help promote the school's e-Safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of e-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the e-Safety coordinator • To maintain an awareness of current e-Safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices.

	• To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand 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 • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • To help the school in the creation/ review of e-Safety policies and children's Acceptable Use Agreement
Parents / Carers	• To support the school in promoting e-Safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic images • To read, understand and promote the school Pupil Acceptable Use Agreement with their children • To access the school website in accordance with the relevant school Acceptable Use Agreement. • To consult with the school if they have any concerns about their children's use of technology
External Groups	Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

5. THE CURRENT TECHNOLOGIES

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include: (examples in brackets)

- The Internet
- E-mail (Office 365, Gmail, BBM Messenger etc)
- Instant messaging often using simple webcams (FaceTime, Skype, Snapchat)
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Twitter, Facebook, Instagram, Snapchat, Club Penguin etc)
- Video broadcasting sites (Youtube, blogs etc)
- Chat rooms (teenchat)
- Gaming sites (Xbox/Playstation online gaming, Neopets)

- Music download sites Mobile phones with camera and video functionality
- Mobile technology (e.g. games consoles or Applications on a device) that are 'Internet ready'
- Smart phones with e-mail, web functionality and cut-down 'Office' applications

6. MANAGING E-SAFETY RISKS

Internet Access

6.1 The Internet is an essential element of education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

6.2 Internet use is a part of our curriculum and a necessary tool for staff and pupils.

6.3 The school Internet access will be designed expressly for pupil use and will use appropriate filtering system.

6.4 Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use. Pupils will not use the internet without having permission from a member of staff.

6.5 Pupils will have controlled access to social networking sites while in the academy and will also be educated about using such sites safely in their own time.

6.6 Pupils will be advised never to give out personal details of any kind, which may identify them, their friends or their location.

6.7 Pupils are forbidden from downloading games or other programs from the internet.

6.8 The ICT Technician will carry out downloading programs from the internet.

6.9 Public chat-rooms and instant messaging are not allowed and are blocked using the Internet filter.

6.10 Access to peer-to-peer networks is forbidden in the school (uTorrent etc.)

6.11 Pupils will be educated in 'Information Literacy' and taught how to evaluate the internet content that they have located. Pupils will be taught the importance of crosschecking information before accepting its accuracy.

6.12 The school will ensure that the use of internet derived materials by staff and pupils complies with copyright laws. Pupils will be taught to reference materials they have found from other sources so as not to infringe copyright or intellectual property of others.

6.13 Pupils will be taught how to report unpleasant internet content.

Published Content and the School Website

6.14 Staff or pupils' personal contact information will not be published. The contact details given online should be the school office. Specific staff information may be published but this will be passed through the Headteacher to verify.

6.15 The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

6.16 Permission from parents or carers will be obtained before photographs of pupils are published on the school website. Pupil's full names will not be used anywhere on the website or Blog, particularly in association with photographs.

6.17 Work can only be published with the permission of the pupil and parents.

6.18 Pupil image file names will not refer to pupil by name.

6.19 Pupil image files should be securely stored on the school network

Video Conferencing and Webcam Use

6.20 When available, video conferencing and webcam use will be appropriately supervised.

6.21 Only use school approved conferencing software.

6.22 Pupils will be taught the dangers of using webcams outside of the school.

Portable Devices

6.23 Mobile phones are not to be used in the school; for children who walk home alone then they are to be left at the school office at the beginning of each day. The sending of abusive of inappropriate text messages is forbidden.

6.24 Staff should not use their personal mobile phones to contact pupils or capture photographs of children. Alternative equipment will be provided by the school.

6.25 Pupils are taught how to protect themselves from being victims of theft and how to report such an event to the correct authority.

Other Devices

6.26 New technologies will be examined for educational benefit and a risk assessment will be carried out before use in the school is allowed.

6.27 Games machines including the Sony PlayStation, Microsoft Xbox and others have Internet access, which may not include filtering. These may not be used in the school. The school's E-Safety strand within the computing curriculum ensures that every pupil is educated about safe and responsible use. Pupils are taught how to control and minimise online risks and how to report a problem through a range of activities that are flexible, relevant and engage pupils' interest.

7. STRATEGIES TO MINIMISE THE RISKS

Key Stage One includes the children being able to:

- Recognise common uses of information technology **beyond school**
- 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
- Understand what to do if they suffer from online peer-to-peer abuse through the use of the Internet

Key Stage Two includes the children being able to:

- Understand computer networks including the Internet; how they can provide multiple services, such as the world wide web; and the opportunities they offer for **communication and collaboration**
- Use search technologies effectively, appreciate how results are selected and ranked, and be discerning **in evaluating digital content**
- Use technology **safely, respectfully and responsibly**; recognise **acceptable/unacceptable behaviour**; identify a range of ways to **report concerns about content and contact.**

8. HOW WILL COMPLAINTS REGARDING E-SAFETY BE HANDLED?

The school will take all reasonable precautions to ensure e-Safety. However, owing to the nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school can not accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements and possible sanctions.

- Interview / Head of Year / e-Safety Coordinator / Head teacher;
- Informing parents or carers;
- Removal of Internet or computer access for a period
- Referral to the Police.

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head teacher. Complaints of cyber bullying are dealt with in accordance with our Anti-Bullying Policy.

Complaints related to child protection are dealt with in accordance with school child protection procedures.

9. HOW WILL THE POLICY BE DISCUSSED WITH STAFF?

It is important that all staff feel confident to use new technologies in teaching. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies.

Staff must understand that the rules for information systems misuse. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their head of year or the e-Safety Co-ordinator to avoid any possible misunderstanding.

ICT use is widespread and all staff including administration, governors and support staff should be included in appropriate awareness raising and training. Induction of new staff should include a discussion of the school's E-Safety Policy.

10. HOW WILL PARENTS' SUPPORT BE ENLISTED?

Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school may be able to help parents plan appropriate supervised use of the Internet at home.

- Internet issues will be handled sensitively and parents will be advised accordingly via e-Safety meetings, leaflets and relevant information on the school website.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

11. E-SAFETY TERMINOLOGY

Acceptable Use Policy: A policy that a user must agree to abide by in order to gain access to a network or the Internet. In the schools context, it may also cover how other communications services, such as mobile phones and camera phones, can be used on the school premises.

Avatar: A graphic identity selected by a user to represent him/herself to the other parties in a chat-room or when using instant messaging.

Chat-Room: An area on the Internet or other computer network where users can communicate in real time, often about a specific topic.

Filtering: A method used to prevent or block users' access to unsuitable material on the Internet.

Information Literacy: The ability to locate pertinent information, evaluate its reliability, analyse and synthesise it to construct personal meaning and apply it to informed decision making.

Instant Messaging (IM): A type of communications service that enables you to create a kind of private chat room with another individual in order to communicate in real time over the Internet, analogous to a telephone conversation but using text-based, not voice-based, communication.

Peer-To-Peer (P2P): A peer-to-peer network allows other users to directly access files and folders on each other's computer. File sharing networks such as 'Lime Wire' creates weaknesses in networks security by allowing outside users access to the schools resources.

Spam: Unsolicited junk email. The term is also used to describe junk text messages received via mobile phones. A related term, spim (or spIM), describes receiving spam via instant messaging.

Spoofing: Assuming the identity of someone else, using an email address either guessed or harvested from repositories of valid email addresses (such as the address book of a virus-infected computer). Spoofing is typically practised to veil the source of virus-laden emails or, often, to obtain sensitive information from spam recipients, without revealing the source of the spammer.

Trojan Horses: A virus, which infects a computer by masquerading as a normal program. The program contains additional features added with malicious intent. Trojan horses have been known to activate webcams, for example, without the knowledge of the PC user. Video Conferencing: The process of conducting a conference between two or more participants over a network, involving audio and often text as well as video.

Virus: A computer program that enters a computer, often via email, and carries out a malicious act. A virus in a computer can corrupt or wipe all information in the hard drive, including the system software. All users are advised to guard against this by installing anti-virus software.

Webcam: A webcam is a camera connected to a computer that is connected to the Internet. A live picture is uploaded to a website from the camera at regular intervals, typically every few minutes. By looking at the website you can see what the camera sees – almost as it happens.