William Cassidi Church of England Primary School

E-Safety Policy Statement

'Life in all Fullness'
(John 10:10)

As a school, we want to provide children with the very best education. To let them experience life in all its fullness and living with all their heart. Our main core value of love underpins all that we do. Our school is Christ-centred and our core Christian values of love, respect, courage, service and resilience flow through every aspect of school life. It is on this bedrock that we provide an excellent education for the children who attend our school. We want every child to be the very best that they can be and to recognise that they are precious, loved and valued.

Introduction

Children and young people are growing up in a digital world. As they grow older, it is crucial that they learn to balance the benefits offered by technology with a critical awareness of their own behaviour and the behaviour of others online. Children must develop effective strategies for staying safe and making a positive contribution online. Our vision is to ensure that children live a 'life in all fullness'. We therefore need to ensure that pupils are well equipped for the wider world so that there are no limitations to what they can achieve. We want children to know how to use technology efficiently, safely and responsibly to become he best that they can be.

"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal. "To ignore e-safety issues when implementing the requirements of Every Child Matters could ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable."

(Taken from: Safeguarding Children in a Digital World. BECTA)

E-Safety Core Areas

Within the school's E Safety support (for its staff and pupils) it focuses specifically on eight different aspects of online education:

1. Self-image and Identity
2. Online relationships
3. Online reputation
4. Online bullying
5. Managing online information
6. Health, wellbeing and lifestyle
7. Privacy and security
8. Copyright and ownership

At William Cassidi C of E Aided Primary School, we recognise that learning is a life-long process and that e-learning is an integral part of it. Ensuring that we provide pupils with the skills to make the most of information and communication technologies is an essential part of our

ethos and curriculum. The school aims to support and broaden the provision of online safety education, so that it is empowering, builds resilience, respect and effects positive culture change for all. However, as in any other area of life, children are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities which are inappropriate, or possibly illegal. E-Safety seeks to address the issues around using these technologies safely and promote an awareness of the benefits and the risks.

This policy sets out clearly the expectations of pupils, staff, parents/carers and members of the wider community to ensure best practice.

E-Safety Co-Ordinators

The day-to-day operational duty of E-Safety Co-Ordinator is devolved to Mr M. Proud. This role is strategically supported by Mrs Campbell in her role as safeguarding lead.

The E-Safety Operational Co-Ordinator will:

- Keep up to date with the latest risks to children whilst using technology; familiarize himself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, governing body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make himself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that the IT technical infrastructure is secure; this will include at a minimum:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Any e-safety technical solutions such as Internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Headteacher
- Passwords are applied correctly to all users regardless of age

Staff Responsibilities

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any e-safety incident is reported to both the e-safety co-ordinator (Mr Proud) and safeguarding lead (Mrs Campbell). An E-Safety Incident Report must be made. This form is readily available on the safeguarding operational board in the staffroom and in a digital format.
- The reporting flowcharts contained within this e-safety policy are fully understood.

Pupil Responsibilities

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

E-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly, all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers Responsibilities

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, school newsletters and any specialist workshops, the school will keep parents up to date with new and emerging e-safety risks and will involve parents in strategies to ensure that students are empowered. Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded.

Technology

Our School uses a range of devices including PC's, laptops and Ipads. In order to safeguard all students and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use Smoothwall software that prevents unauthorized access to illegal websites. This filter is designed to prevent accidental or deliberate access to unsuitable materials. Smoothwall monitors the contents of all websites rather than just the type of site. The school uses a layering system of authorisation comprising of three categories; pupil, teaching staff and MIS/Admin. Designated restrictions are placed on each to ensure that highest level of e-safety possible. The filter logs and retains evidence of individual usage over a six-month rolling period and records can be obtained throughout that time. If there are any concerns the E-Safety Officer and Headteacher are able to monitor any person's activity directly.

The ICT Coordinator and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher. Records of which iPads children are using will be kept so appropriate feedback can be provided to the correct child in case of any misuse of internet access.

Email Filtering – we use software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are password protected. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are password protected. For added protection of any personal data no such information will be taken away from school and staff will use Remote Access rather than USB Keydrives. Any breach (i.e. loss/theft of device such as laptop) is to be brought to the attention of the Head Teacher immediately. The Head Teacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

Passwords – all staff and students will be unable to access any device without a unique username and password. The ICT Coordinator and IT Support will be responsible for ensuring that students from Y2-Y6 use unique passwords.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out and will report to the Headteacher if there are any concerns. All USB peripherals such as keydrives will to be scanned for viruses before use.

Safe Use of Technology for Pupils

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy. There are many social networking sites available for the children to access via the Internet. William Cassidi Primary School takes the responsibility of discussing the risks involved very seriously.

Email/Instant Messaging Safety - Some pupils will have their own webmail accounts at home. As these are independent of the school they do not necessarily come with the safeguards that we set for email usage. Therefore, we do not permit the use of personalised email accounts by pupils at school or at home for school purposes. We provide regular safety notices / advice to parents and carers regarding their monitoring of their child's accounts and keeping their children safe online.

E Safety Ambassadors

- Individual children within school who have shown a responsible attitude to e-safety act as 'E-safety Ambassadors'. Their role is to review the school's e-safety rules, run special e-safety promotion days, be a good role model to other pupils and liaise with any pupil with e-safety concerns and the e-safety Coordinator and/or Headteacher
- When Appropriate the E-Safety Ambassadors will join with the KS2 School Councillors to promote anti-bullying in all areas as well as keeping each other safe both around school and on the Internet
- All National internet safety days or anti-bullying days will be observed in order to constantly address/remind staff and pupils of these issues.

Safe Use of Technology for Staff

Email – All staff are reminded that emails are subject to Freedom of Information requests and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Photos and videos – Any data processing of digital images is done in line with Data Protection Act 2018 (DPA), General Data Protection Regulation (GDPR) and the school's relevant policy. If considered necessary a Data Protection Impact Assessment (DPIA) will be carried out.

Digital still and video recording devices are used for recording special events as well as being essential tools for everyday learning experiences across the curriculum. As part of pupil induction and yearly thereafter, parents/carers are asked to sign a consent form for images of their children to be used for school purposes. Some images celebrating the work of pupils involved in everyday and special event activities may be selected to be shown on the school website, the school's e-learning platform, social media platforms or marketing materials. For GDPR and safeguarding purposes we never state a child's full name with their image. The relevant GDPR consents are issued annually. GDPR consents request individual permissions per platform.

Digital images may be shared with partner schools and organisations as part of collaborative learning projects. This can include live video conferencing. All such use is monitored and supervised by staff. Parents/carers provide GDPR consent for this.

Social Networking – there are many social networking services available; school is fully supportive of social networking as a tool to engage and collaborate with learners and to engage with parents and the wider school community. The following social media services are permitted for use within school and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the e-Safety Co-ordinator who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Eschools – used by staff and students in schools
- Eschools Mail - used by the school as a home/school communication platform
- Facebook – used by the school as a marketing platform and broadcast service for the local community
- X – used by the school as a marketing platform and broadcast service for the wider educational community.

In addition, the following is to be strictly adhered to:

- GDPR permissions must be approved before any image or video of any child is uploaded
- There is to be no identification of students using full their full name
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Online Relationships

Pupils will learn through Computing, PSHE, SMSC and collective worship that people sometimes behave differently online, including by pretending to be someone they are not. The above curriculums also fulfil the schools 'due regard' responsibilities under the 'PREVENT' initiative

to protect children and young people from being drawn into extremism via online content and online relationships.

Pupils will learn:

- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous;
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact and how to report them;
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online.

Incidents - Any e-safety incident is to be brought to the immediate attention of the E-Safety Co-Ordinator and the Headteacher / safeguarding lead. The E-Safety Co-Ordinator will assist staff in taking the appropriate action to deal with the incident and to fill out an incident log. The incident log must be submitted to the Headteacher / Safeguarding lead.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. E-Safety for pupils is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the pupil's learning. As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The E-Safety Co-Ordinator is responsible for recommending a programme of training and awareness for the school year to the Headteacher for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

The School Website

The school website contains school policies, newsletters and other information. We expect all persons accessing the school website to treat the content with respect and make no attempt to reproduce, use or alter any part in any way with malicious intent. No part can be reproduced for commercial reasons without written permission from the school.

Physical Safety

- All electrical equipment in the school is tested annually to ensure that it is safe to use. We expect pupils to behave appropriately near electrical sockets and appliances
- Workstations are cleaned and sanitised regularly. We expect all users to refrain from eating and drinking when working at a computer. Health and safety guidance states that it is not healthy to sit at a computer for too long without breaks. The school now has various portable devices, for example Ipads, cameras, microscopes, microphones and metal detectors. The teacher will instruct users on how to manage this equipment safely on a time-by-time basis. We expect all users to use great care when moving around with such items in order that they do not harm themselves, others or the device itself.

Staff Use of Social Media Platforms and Digital Footprint

Staff online communication with children attending William Cassidi C of E Primary school and/or those who have previously attended (but are under the age of 16) is forbidden. If any member of staff is found to be doing such then this will instigate disciplinary proceedings. Whereby there is an existing relationship via social media between a colleague and a parent / carer of an existing pupil (or previous pupil under the age of 16) there must be a disclosure form completed and submitted to the Headteacher for safeguarding purposes. This process safeguards staff against any potential allegations.

From September 2022 changes came into effect, via KCSIE, regarding online searches of staff during the recruitment process:

'In addition, as part of the shortlisting process, schools and colleges should consider carrying out an online search as part of their due diligence on the shortlisted candidates. This may help identify any incidents or issues that have happened, and are publicly available online, which the school or college might want to explore with the applicant at interview.'

(NASUWT – October 2024)

Staff must be aware of their digital footprint and responsible use of social media platforms in line with the above recruitment processes and part two of teacher standards: professional conduct.

Cyberbullying

The school takes all forms of bullying very seriously and has robust procedures for identifying and dealing with it. Cyberbullying is the use of any communication medium to offend, threaten, exclude or deride another person. This can be in relation to their friends, family, gender, race, culture, ability, disability, age or religion. We also raise awareness of the impact of bullying, responsibilities of bystanders (primarily reporting bullying to an adult) and how to get help. We expect all members of our community to communicate with each other with respect and courtesy. Bullying of any type will not be tolerated by the school and will be dealt with under the procedures within the Whole School Policy on Behaviour.

Mobile Phones

Pupils are not permitted to have mobile phones upon their person in school. We recognise that our oldest pupils may walk on their own to and from school and parents may wish them to have a mobile phone for emergencies. However, we discourage this on security grounds as they are easily lost, damaged or stolen. The use of any mobile phones, which have the ability to take photographs, is forbidden within the school premises except for those used by parents/carers within the school hall for the purpose of taking pictures of their child/children during family worship or school productions. The Headteacher / safeguarding lead also has access to a school phone, which is used for marketing purposes and as an absence line. The school logo is visible on the outside of the

phone case to avoid any confusion regarding the use of a personal device.

All visitors will be requested to turn off their phones at Reception with the exception of the One IT technician, who requires his device in order to carry out his job.

School staff will only use their personal mobiles within the appointed staffroom area, which is positioned opposite Class 3.

The school will provide an appropriate device to use on educational visits.

Other technologies:

> Podcasting – Some pupils will be given opportunities to create oral recordings. Some of these recording may be made available as podcasts through the Internet so that they can be shared with interested members of the school community.

Copyright:

Though there are lots of free to use resources on the Internet, the majority of image, sound and music files are covered by copyright laws. Some can be used for educational reasons without permission provided that the source is stated and that they are not made available outside the school. Some cannot be used under any circumstances, this is particularly so for music but can apply to other types of file e.g. photographic images. Care therefore needs to be taken with multi-media work which incorporates anything downloaded from the Internet or any other published source that it is not uploaded onto the school's website or broadcast through any other technology. *Pupils are taught that the people who put their work on the Internet may not always want people to copy or use their work and that they should check whether they have permission.* We expect all users to respect copyright laws.

This policy will be reviewed annually or earlier if appropriate.

Policy approved by the Governing Body: October 2024
Date of review: October 2025

E-Safety Rules for KS1

Think then Click
These rules help us to stay safe on the Internet
1. We tell our teacher or Mr Proud if anything on the computer makes us sad or worried. 2. I will listen carefully to instructions when in the ICT Suite. 3. I will be polite and behave well on the computer. 4. I will only use the computer when my teacher tells me to and there is an adult present. 5. I will use the programme or website that my teacher wants me to.

E-Safety Rules for KS2

I promise – to only use the school ICT for schoolwork that the teacher has asked me to do.
I promise – not to look for or show other people things that may be upsetting.
I promise – to show respect for the work that other people have done.
I will not – use other people's work or pictures without permission to do so.
I will not – damage the ICT equipment, if I accidentally damage something I will tell Mr Proud or my teacher.
I will not – share my password with anybody. If I forget my password I will let Mr Proud or my class teacher know.
I will not – use other people's usernames or passwords.
I will not – share personal information online with anyone.
I will not – download anything from the Internet unless my teacher has asked me to.
I will – let Mr Proud or my teacher know if anybody asks me for personal information.
I will – let Mr Proud or my teacher know if anybody says or does anything to me that is hurtful or upsets me.
I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell Mr Proud or my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Student):

Date :

E-Safety Incident Log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head, e-Safety Officer)*	
	When:	**When:**	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review Date:			
Result of Review:			
Signature: (Head Teacher)		**Date:**	