Holywell C of E Primary School

Online Safety Policy

Flowing, Strengthening, Deepening

Approved by:	FGB	**Date:**	January 24
Last reviewed on:	January 23		
Next review due by:	January 25		

Background to this Policy

The purpose of this policy is to describe the safeguarding measures in place for adults and children in school with relation to online safety, including:

- **The policies and practice embedded in our school and followed by the whole school community.**
- **The infrastructure and how it is set up to keep pupils safe online, including filtering, monitoring and preventing and responding to online safety incidents.**
- **A progressive, relevant age-appropriate online safety curriculum for all pupils which (as a minimum) meets the requirements of the National Curriculum for Computing and the statutory Relations and Health Education.**

Online safety in schools is primarily a safeguarding concern and not a technology one. There, this policy should be viewed alongside other safeguarding policies and approaches including, but limited to:

- **Safeguarding and Child Protection**
- **Personal Social and Health Education (PSHE)**
- **Data Protection/GDPR**
- **Anti-Bullying Policy**
- **School Complaints Procedure**
- **Whistle Blowing Policy**
- **Mobile Phone and Smart Device Policy**
- **Cambridgeshire Progression in Computing Capability Materials**

This policy should be read alongside the staff and pupil Acceptable Use Policies (AUPs).
These AUPs outline the expectations and sanctions which apply to staff and pupil use of technology.
The development of our online safety policy involved:

- **The Headteacher/DSL**
- **The Computing Subject Lead**
- **The Governor responsible for Safeguarding**

Rationale

At Holywell Church of England Primary School, we believe that the use of technology in education 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 exciting and innovative technology tools in school and at home has been shown to support learning and promote pupil achievement. Yet at the same time, we recognise that the misuse of technology can put users at risk within and outside the school.

The risks they may face can broadly be categorised into the 4 C's; **Contact, Content, Conduct and Commerce.** (the latest version of the Keeping Children Safe in Education document) and may include:

- Access to harmful, illegal or otherwise unsuitable content including gaming, gambling sites, sexually explicit material and websites with extremist ideologies and images.
- Unauthorised access to/loss of/sharing personal information
- The risk of being subject to grooming by those with who, they make contact on the internet, including the sharing of Self-Generated Indecent Images.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others
- Cyber-bullying
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading or streaming of music or video files
- Phishing or financial scams
- 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 just to them. Online safety issues can also affect adults who work or are associated with the school and this will be referenced later in this policy.

Technologies regularly used by pupils and staff include:

Staff:

- Staff laptops/Staff Class I pads (Password protected) – staff devices can also be used at home in accordance with the staff AUP, particularly with regard to GDPR.
- Peripheral devices e.g. Interactive whiteboards
- Staff level internet access
- Personal devices should not be connected to the school WIFI without permission from the Headteacher.

Pupils:

- IPads – filtered access to the internet, accessed through Smoothwall Browser for monitoring purposes
- Laptops – Laptops password protected, either single user (no access to school network) or class password (very limited access to school network i.e., class files only). NB at present this is not used and laptops are used as an alternative device for accessing the internet. Devices are signed out by pupils when used and monitored through Smoothwall.

Where the school changes the use of existing technologies or introduces new technologies which may pose risks to user's safety, a risk assessment will be completed to show how the risk is being mitigated and reduced to an acceptable level.

The Online Safety Curriculum

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 situation which make them feel uncomfortable. The need for a progressive, age-appropriate online safety curriculum is clearly documented in the National Curriculum for Computing (England) and the statutory Relationship and Health Education.

At Holywell CofE Primary School we believe that a comprehensive programme of online safety education is vital for developing our pupils' ability to use technologies safely. 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 a range of online services including the World Wide Web.

Our online safety curriculum is based on the Cambridgeshire Progression In Computing Capability Materials (Appendix 1) and the Cambridgeshire PSHE Service Primary Personal Development Programme, with reference to UKCIS's Education for a Connected World.

Aims of School Internet and Email access

School internet and email access should be used by staff to:

- Raise educational standards
- Support curriculum development
- Support staff professional development
- Enhance communication and the exchange of data between schools, the Local Authority and government departments
- Enhance professional communication and administration within school
- Enhance communication and information sharing between school and parents/carers (e.g., use of Seesaw)

School internet access should be used by pupils where:

- Internet access is planned to enrich and extend learning activities as an integrated aspect of the curriculum
- Pupils are given clear learning objectives for Internet use
- Pupils are provided with relevant and suitable web sites and resources
- Pupils will be made aware that the author of a web page, email or text message may not be the person they claim to be, and are taught to validate information before accepting it as true
- Pupils are taught to observe copyright when copying materials from the web and to acknowledge their sources of information
- Pupils are taught to expect a wider range of content than is found in other media sources
- Pupils access the internet, on IPads, through Smoothwall Browser to help facilitate monitoring of device use

These aims are achieved by using a combination of:

- **Discrete and embedded activities drawn from a selection of appropriate materials and is linked to demonstrating safe practice in our online learning platform. These include the teaching of the 'SMART' rules, Jessie and Friends and Bandrunner.**
- **Key online safety messages are delivered and reinforced through cross curricular opportunities such as emailing, researching, blogging and communicating in appropriate online environments.**
- **Focus events to raise the profile of online safety for our pupils and school community.**
- **A flexible curriculum which is able to respond to new challenges as they arise.**

Continued Professional Development

Staff at Holywell receive up to date information and training on online safety in the form of staff meetings and updates from the school's online safety and Designated Safeguarding Leads, as well as training from external providers where appropriate.

Nominated members of staff will receive more in-depth training to support them in keeping up to date and reviewing the school's approach, policies and practice.

New staff receive information on the school's acceptable use policy as part of their induction, including advice on Protecting their Professional Reputation Online.

All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.

Mobile Phones and Use of Mobile Data in School

The latest version of Keeping Children Safe in Education acknowledges that "many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e., 3G, 4G and 5G)."

See Mobile Phone Policy

Acceptable Use of Internet and Email

- The use of ICT resources will be for directed purposes on the basis of educational and administrational need
- Users will access and amend files and documents using their password which will be confidential at all times
- Hardware encrypted memory sticks will be used to store and transfer information
- School data may not be transferred onto any equipment not owned by the school
- The Headteacher and Governing Body reserves the right to look at all files on the school system and approve access by users
- Any user of the school e-mail systems must not communicate inappropriate or offensive material.

Monitoring and Averting Online Safety Incidents

- County firewall software provides anti virus protection
- Filtered access for both adult and child use is provided by the County Internet Service Provider
- All Internet access by pupils is supervised by a member of staff or other responsible adult
- Staff should not communicate with pupils in the school through social networking websites
- Staff should teach pupils to adhere to the age restrictions of social networking websites
- No pupil, member of staff or community user is permitted to access material that is illegal or potentially offensive using school systems
- The copyright and intellectual property rights of material using the school system will be respected
- All staff have received training in GDPR
- All staff and pupils have a responsibility to report e safety or e security incidents
- Smoothwall browser installed on pupil IPads. All KS2 children keep a personal device log to record details of device use. In KS1 teacher will keep a log of devices used by children.
- Use of Staff laptops is monitored and any inappropriate use reported to the Headteacher.
- Head teacher receives a weekly report of any inappropriate searches.

Online Safety Education

Children are taught online safety across the school through assemblies, 'Safer Internet Days', PSHE, posters and Computing lessons (including dedicated E-Safety lessons). SMART guidance is taught and shared with children:

Safe: Keep safe by being careful not to give out personal information when chatting or posting online. Personal information includes your email address, phone number and password.

Meeting: Meeting someone you have been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

Accepting: Accepting emails, messages, or opening files, pictures or texts from people you don't know, or trust can lead to problems- They may contain viruses or nasty messages.

Reliable: Someone online might lie about who they are, and information on the internet may not be true. Always check information with other websites, books or someone who knows.

Tell: Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or you or someone you know is being bullied online.

Responding to Incidents

It is important that all members of staff are aware of how to respond if an e-safety incident occurs or if they suspect a child is at risk through their use of technology. (See Appendix 2)

- Responses to e-safety incidents will be consistent with other incidents in school.
- If an e-safety incident occurs, the school will follow its agreed procedures for dealing with incidents including internal sanctions and involvement of parents.
- Where the school suspects that an incident may constitute a Child Protection issue, the usual Child Protection procedures will be followed.

Digital Publishing

The school has its own web site. Ultimate responsibility for the content of the site rests with the Headteacher in line with the following guidelines

- Parent / carer permission will be sought before publication of photos, videos and DVDs generated or identified by the school
- Personal information will only be published with parent / carer permission
- Individual pupils will not be identifiable by full name at any time
- Parents are advised that photographs including images of other pupils at school events, e.g., plays, sports day, should not be put into the public domain, e.g., social networking websites

Mobile IT hardware e.g., laptops and IPads in transit

- Mobile IT resources are to be stored in a locked compartment e.g., car boot when in transit (insurance requirement).
- Mobile IT resources e.g., laptops are to be used exclusively for school purposes.

Disposal of hardware

- All obsolete hardware will be safely and securely disposed of
- All obsolete hard drives will be wiped prior to safe disposal.
- PRM Green Technologies (can collect from all 3 schools across the federation for redundant educational equipment)

Adoption and annual review of the Online Safety Policy

This policy was adopted at a meeting of:	Full Governing Board
Held on:	18th January 2024
Print name: **Signed on behalf of the FGB:**	Alan Whitaker Alan Whitaker

Cambridgeshire Progression in Computing Capability

These progression statements are designed to complement the National Curriculum for Computing in England. More detailed guidance for both **subject leaders** and **class teachers** can be found at www.theictservice.org.uk/primary-computing

	Understanding Technology	Programming	Digital Literacy	Online Safety
Year 1	Pupils recognise and can give examples of common uses of **information technology** they encounter in their daily routine.	Pupils create, **debug** and implement instructions (simple **algorithms**) as **programs** on a range of digital devices. Pupils understand that **digital devices** follow precise and unambiguous instructions. They understand that digital devices can **simulate** real situations.	With adult guidance, pupils use a range of technology to enhance and present their learning. Within both specific computing lessons and cross curricular contexts, pupils are able to: • enquire with purpose, accessing **digital content** such as text, still and moving images, video and audio • collect **data** (e.g., numerical, research facts etc.) which they are able to retrieve, store and present as graphs, tables and charts • present and communicate their learning to others in a variety of ways using text, still images, video and audio, including combining 2 or more of these mediums	Pupils are becoming increasingly aware of **content**, **contact** and **conduct** benefits and risks, how to manage them safely and where to go for help and support when they have concerns or feel unsafe, worried or upset. They are beginning to develop a better understanding of their own and others' **'identity'** (including online), the importance of keeping personal information private and of seeking permission before sharing. They check with an adult before clicking on **pop ups**, **notifications** or **dialogue boxes**. They increasingly use a range of **digital devices** to communicate safely and respectfully online, making links to positive behaviour in the physical world. *More specific guidance for Year 1 and Year 2 teachers can be found at www.theictservice.org.uk/primary-computing*
Year 2	Pupils recognise common uses of **information technology** beyond school, including those which they don't frequently encounter in their daily routine. Pupils understand that computers are not intelligent but can appear to be when following **algorithms**. They can share examples of this.	Pupils understand that **algorithms** are implemented as **programs** on **digital devices.** Pupils create and **debug programs** to achieve specific goals and understand the importance of **sequence**. Pupils use the **principles of logical reasoning** to plan and predict the behaviour of simple **programs**. They solve problems on and off screen		
Year 3	Pupils understand that **computers** (in various forms) generally accept **inputs** and produce **outputs** and can give examples of this. Pupils recognise - and can describe - some of the services offered by the **Internet**, especially those used for communication and collaboration.	Pupils create **programs** to accomplish specific goals using an increasing range of **digital devices** and **applications**. They can **decompose** programs to test them and understand how making even small changes to an **algorithm** can have a significant impact on the outcome. They begin using **simple repetition** (e.g. *'repeat x times'* and *'repeat forever'*) and understand how this can be used to improve **efficiency** in their programs.	With increasing levels of autonomy, pupils are becoming confident and creative users of technology. Within both specific computing lessons and cross curricular contexts, pupils are able to: • follow and expand on agreed lines of enquiry, using key words and phrases to effectively access **digital content** such as text, still images, video and audio • identify, collect and manipulate different types of **data** (e.g. numerical, research facts etc.) which they present as **information**, showing a greater awareness of purpose and audience • present and communicate their learning to others in a variety of ways using text, still images, video and audio • They combine **digital tools** to achieve **specific goals** and think carefully about the **impact on their audience**	Pupils are able to identify a range of **content**, **contact** and **conduct** benefits and risks, describe how to manage them safely and respectfully and know where to go for help and support when they have concerns. They can explain what is meant by **'identity'**, how this might be represented differently in different situations and why others might mis-represent their identity. They develop their understanding of **'trust'** and the importance of being careful about what is shared online and of giving and gaining **consent**. Pupils can describe **positive and negative effects of online activity / behaviours** and begin to understand how to make safer and healthier decisions, including considering the appropriateness of games and online content for different ages. Pupils can describe positive ways for someone to interact with others online and understand how this will positively impact on how others perceive them. *More specific guidance for Year 3 and Year 4 teachers can be found at www.theictservice.org.uk/primary-computing*
Year 4	Pupils develop a basic understanding of how computers can be linked to form a **local network** such as those found in schools. Pupils recognise that there is a difference between the **Internet** and the **World Wide Web.** They can recognise and describe some of the services offered by the **Internet**, especially those used for communication and collaboration.	Pupils create and debug **programs** containing **simple repetition** (e.g. *'repeat x times'* and *'repeat forever'*) as well as more **complex repetition** (e.g. *'nested loops'*) Pupils increasingly use their programming capability to control or simulate a range of different **outputs** in **physical systems.** Pupils begin to explore and notice the similarities and differences between **programming languages** and use this knowledge to help them create and **debug programs** efficiently.		
Year 5	Pupils know that there is a difference between the **Internet** and the **World Wide Web** and understand that the web is just one of the services offered by the Internet (as well as, e.g. **email** and **VoIP services** such as Skype). They appreciate how **search results** are ranked, including an understanding of the use of different **algorithms** to prioritise results. Pupils understand that the highest-ranking search results may not always be the most relevant. They appraise search results based on their **relevance** and **trustworthiness**, and can explain what is meant by '**fake news**'	Pupils create, **deconstruct** and refine **programs** to accomplish specific goals. They create programs with **loops** which terminate when **conditions** are met or continue whilst **conditions** are present (e.g. *'repeat until' and 'repeat whist'*). Pupils understand and use simple **selection** (e.g. *if/then* and *if/then/else*) to create **interactive programs** based on **conditions** being met / not met. They begin to use simple **operators** within their programs.	Pupils are confident, capable and creative users of technology. Within both specific computing lessons and cross curricular contexts, pupils are able to: • create and effectively follow lines of enquiry to support their learning, and are discerning in **evaluating digital content** they encounter • identify, collect and analyse different types of **data** (e.g. numerical, words, images, video etc.) which they manipulate and re-present as **information** for a variety of audiences and	Pupils identify and manage the benefits and risks of a range of online activities in terms of **content**, **contact** and **conduct** to ensure they are **safe**, **respectful** and **responsible** online. They know how to report concerns, seek support for themselves and others and persist until they get the help they need. Pupils make responsible choices about their own online **identity** and consider the potential impact of this on their **digital footprint.** They understand that online **identities** can be **copied** or **modified** and some of the possible implications of this. They can describe times when they might responsibly share

Year 6	Pupils understand and can explain how **computer networks** work, including the **Internet.** They begin to understand how **data** travels across **networks** in **packets** and how these can be broken up and reconstructed. When accessing information online, pupils recognise that **opinions** may be presented as **facts.** They can describe why an opinion may easily become popular online but they understand that this doesn't necessarily make it true. They understand that some online content may be commercially sponsored such as **adverts in search results** or content presented by **social media influencers**.	Pupils create, **deconstruct** and refine an increasingly complex range of **programs** to accomplish specific goals. Pupils create **programs** which store, change and report **variables** (e.g. scores in a game or time) and can include multiple **variables** in a single **program**. Pupils can explain why they have structured **algorithms** as they have and describe the effect this has on a **program**.	purposes • select and make effective use of **digital tools** to create **digital artefacts** both under instruction and of their own choosing • decide on the most appropriate way to present their learning - thinking about **aesthetics**, **functionality** and **impact** on the user, and responding appropriately.	**personal information** (including payment details), the importance of seeking permission and the need for **strong passwords**. They can describe ways technology may impact their own and others' **physical and mental wellbeing** (positively and negatively), understand their responsibilities in regard to this and can suggest a range of positive strategies to limit the negative impact of technology and online behaviours. *More specific guidance for Year 5 and Year 6 teachers can be found at www.theictservice.org.uk/primary-computing*

Draft - August 2020

Holywell Cof E Primary School Online Safety Policy

Where the school suspects that an incident may constitute a Safeguarding issue, the usual Safeguarding procedures will be followed. This process is illustrated below.

Figure 1. Responding to a Safeguarding Incident where Technology is Involved