Stratford-sub-Castle Church of England VC Primary School

Life in all its fullness

Online-Safety Policy

The *Online-Safety Policy* was reviewed during the Summer Term 2024. This document is the result of that review. Updated to take into account *Keeping Children Safe in Education* and *Teaching online safety in school (2024).*

DATE AGREED BY FULL GOVERNING BODY:	25.09.24
REVIEW DATE:	**September 2025**
REVIEW CYCLE:	Annually
AUTHOR:	**Miss Katherine Smith**
HEADTEACHER:	**Mrs Justine Watkins**
FGB/COMMITTEE:	**Full Governing Body**
NOMINATED GOVERNOR:	**Mrs Emma Cash/Mrs Nicola Clare**
CHAIR OF GOVERNORS:	**Mr Andrew Mintram**
SIGNED:	*A.Mintram*
TO BE READ IN CONJUNCTION WITH:	***Acceptable Use Policy*** ***Aims of the School*** ***Anti-bullying* Policy** ***Behaviour for Life and Learning Policy*** ***Code of Conduct (for staff, supply and volunteers)*** ***Code of Conduct for School Governors*** ***Complaints Policy*** ***Child Protection* Policy** ***Health and Safety Policy* with its related policies** ***Home School Agreement*** ***Keeping Children Safe in Education*** ***Relationship and Sex Education Policy*** ***Safeguarding Policy*** ***Teaching Online Safety in School*** ***Whistleblowing Policy***

Stratford-sub-Castle Church of England VC Primary School

LIFE IN ALL ITS FULLNESS (John 10:10)

Online-Safety Policy

Our online-safety policy has been written by the school, using the Wiltshire online-safety template policy and government guidance. It has been written in conjunction with the UK Safer Internet Centre guidance and the document 'Keeping Children Safe in Education'.

Introduction

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

The head teacher and Computing subject leaders ensure that this policy is implemented and complied with. The Computing subject Leader is **Miss Kat Smith.** The governors responsible for this area are Mrs Emma Cash and Mrs Nicola Clare.

What is online safety?

Online safety is defined as being safe from risks to personal safety and wellbeing when using all fixed and mobile devices that allow access to the internet, as well as those that are used to communicate electronically.

It means ensuring that children and young people are protected from harm and supported to achieve the maximum benefit from new and developing technologies without risk to themselves or others. This includes personal computers, laptops, mobile phones, tablets, games consoles and any other device that allows access to the internet.

The aim of promoting online safety is to protect young people from the adverse consequences of access or use of electronic media, including from bullying, inappropriate sexualised behaviour, or exploitation.

Safeguarding against these risks is not just a responsibility for Computing Subject Leaders, it is everyone's responsibility, and needs to be considered as part of the overall arrangements in place that safeguard and promote the welfare of all members of the community, particularly those that are vulnerable.

The term 'safeguard' is defined for the purposes of this document in relation to online safety as the process of limiting risks to children when using ICT through a combined approach to policies and procedures, infrastructure, and education, underpinned by standards and inspection.

Online safety policy statement

The purpose of this online safety policy is to:

- Safeguard and protect all members of our school community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.

- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

The main areas of risk for our school community can be summarised as follows:

Content:

- exposure to illegal, inappropriate or harmful material, including online pornography, ignoring age ratings in games (exposure to violence and inappropriate language);
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites;
- hate sites;
- content validation: how to check authenticity and accuracy of online content.

Contact:

- being subjected to harmful online interaction with other users;
- grooming;
- child sexual exploitation
- cyber-bullying in all forms;
- extremism and radicalisation
- identity theft and sharing passwords.

Conduct:

- personal online behaviour that increases the likelihood of, or causes, harm;
- privacy issues, including disclosure of personal information;
- digital footprint and online reputation;
- health and well-being (amount of time spent online (socialising, watching video or gaming));
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images);
- copyright (no thought or consideration for intellectual property and ownership – such as music and film).

Commerce:

- risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

This policy acknowledges that online safety is an essential part of safeguarding and as a school, we have a duty to ensure that all learners and staff are protected from potential harm online.

This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

How will internet use enhance learning?

The use of the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life. We believe that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.

Pupils only access the internet through the schools network. The school internet access is designed expressly for educational use and includes filtering appropriate to the age of the school's pupils. The school ensures that pupils are safe from terrorist and extremist material when accessing the internet.

Pupils at Stratford-sub-Castle Primary School learn appropriate internet use and are given clear guide-lines for internet use. Pupils only use school devices to access the internet – laptops. computers and tablets. Pupils do not use their personal mobile phones or smart technology, ie. smart watch, in school.

How will pupils be taught online safety?

Online Safety and the acceptable use of technology is taught alongside the Computing Curriculum as well as through explicit lessons. We follow the Jigsaw Scheme for our PSHE lessons, which includes Online Safety as an ongoing part of the units taught for all year groups.

Other schemes and resources used are:

- UKCCIS published 'Education for a connected world framework'. Online safety is a whole school and college issue. The framework aims to support the development of the curriculum and is of particular relevance to PSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond and to be central to a whole school or college approach to safeguarding and online safety. It covers early years through to age 18
- The PSHE Association provides guidance to schools on developing their PSHE curriculum – www.pshe-association.org.uk
- Parent Zone and Google have developed Be Internet Legends a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils
- UK Safer Internet Centre website has age appropriate videos and other resources to enable children to discuss how they use the internet and how they can keep themselves safe https://www.saferinternet.org.uk/

We have a 'whole school topic day' to promote Online Safety in February which coincides with the date of Safer Internet Day. This is promoted by the UK Safer Internet Centre.

How will Internet access be authorised?

The school keeps a record of all staff and pupils who are not granted internet access. The record is kept up-to-date. Children are not issued with individual e-mail accounts, but are authorised to use a class email address under supervision, if it is beneficial for educational purposes.

How will filtering be managed?

The school adheres to the DFE filtering and monitoring standards and Cyber Security Standards set out in KCSIE 2023. Our online safety mechanisms are reviewed annually.

The school works in partnership with parents, guardians, Wiltshire Council, Department for Education (DFE), Oakford Technology and the South West Grid for Learning (SWGFL) to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL (internet address) and content must be reported to Oakford via the Computing subject leaders. The filtering system is provided by Oakford Technology. The Computing subject leaders also have access to the filtering password so that they may add unsuitable sites to it immediately. The Computing subject leaders are to complete monitoring of the filtering system, using the UK Safer Internet Centre toolkit, so that we have full knowledge of what our pupils are accessing via the internet and can act on any inappropriate content by immediately blocking. Any concerns are reported to the Headteacher, and then to members of staff.

Managing Content

As a school we ensure that the use of internet derived materials by staff and by pupils complies with copyright law. Specific lessons teach all pupils how to read for information from web resources and decide whether the information is reliable and relevant. The Computing subject leaders are responsible for permitting and denying additional websites as requested by colleagues.

The point of contact on the school's website is the school's address, email and telephone number. In accordance with The Data Protection Act 2018, Staff or pupils' home information is never published. Pupils' full names are not used anywhere on the website, particularly when in association with photographs. Written permission from parents or carers is always obtained before photographs are published on the school website (See *Photo Consent* form). The head teacher has overall editorial responsibility and ensures that content is accurate and appropriate.

New content, e.g. web programs or platforms, that are needed for educational purposes must be set up or downloaded with permission from Oakford. This is to make sure our data is secure in accordance with the GDPR. If any member of staff wishes to access a new program or technology, they must contact the Computing subject leaders who will liaise with Oakford. All new content is added to our audit information.

Safety

Managing email and online communications in school:

Pupils are allowed to access only approved email accounts on the school system, as well as permitted video conferencing platforms, e.g. Skype, and must immediately tell a teacher if they receive offensive mail or other form of contact. Pupils are taught that they must not reveal details of themselves or others in communications with people online; such as their address, telephone number, or arrange to meet anyone. Pupils understand that they are to use email in an acceptable way, follow internet safety rules and will be banned from using the internet in the event of serious breaches of the rules. The use of online chat is not permitted in school, other than as part of its online learning environment, e.g. class blogs. This is closely monitored by the class teacher.

Each year group will have specific online-safety lessons which are outlined on the school curriculum map taken from National Curriculum. However, each class teacher also has the responsibility to plan lessons in response to the specific needs of the children in the class. This is because the school recognises the rapid rate at which technology develops. The older pupils are encouraged to contribute, design and deliver online-safety sessions to younger pupils.

Physical Safety.

The school ensures**,**

- all electrical equipment in the school is tested annually to ensure that it is safe to use. *Pupils are taught about the dangers of electricity as part of the science curriculum.* We expect pupils to behave appropriately near electrical sockets and appliances.
- workstations are cleaned and sanitised regularly. *Pupils are taught to avoid taking food and liquids anywhere near the computers.* We expect all users to refrain from eating and drinking when working at a computer.
- pupils do not to sit at a computer for too long, without breaks. *Pupils are taught correct posture for sitting at a computer and that sitting for too long at a computer can be unhealthy.* We expect all users to take responsibility for their own physical well-being by adopting good practices.
- computers and other ICT equipment are used safely damage prevented. *Pupils are taught the correct way to use ICT equipment.* We expect pupils to respect ICT equipment and take care when handling and using.

Network Safety:

The school ensures that,

- all users are required to log on using a username and password. Pupils log on using a different user name depending on their class group. *Pupils are taught that they should only access the network using that particular log in.* We expect all users to only logon using their username.
- each user is given an allocation of disk space for the storage of their work. *Pupils are taught how to save and retrieve their work into their "My documents" area within their named folder.* We expect pupils to save and keep their work to build up a portfolio of evidence. *Pupils are taught not to access another user's work without permission.* We expect pupils to respect the privacy of all other users and to make no attempt to access or interfere with another user's work.

- only the network administrators are permitted to install software on to computers. *Pupils are taught that the network or an application may not function properly if other programmes are installed.* We expect all users to make no attempt to load or download any programme onto the network.
- all users of the network are monitored remotely by the network administrators. *Pupils are taught that their use of the network can be monitored.* We expect all users to understand that their use is subject to monitoring.

E-Bullying/Cyber Bullying:

The school:

- takes bullying very seriously and has robust procedures for identifying and dealing with it. E-bullying is the use of any communication medium to offend, threaten, exclude or deride another person or their friends, family, gender, race, culture, ability, disability, age or religion. Pupils are taught about bullying as part of learning about emotions and safety.
- expects 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 "Behaviour for Life and Learning Policy" and the Anti-bullying Policy.

Pupils:

- do not have access to any social media or online communication providers whilst in school, except in special circumstances, e.g. contributions to a class blog. These circumstances are monitored at all times by the class teacher and children are only allowed to use designated class logins or email addresses.

Mobile Phones:

The school:

- does not permit pupils to have mobile phones upon their person in school. We recognise that our older 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. Pupils are taught that they shouldn't have a mobile phone on their person in school and that any phone brought in must be handed to the office for the duration of the day. We expect pupils not to carry a mobile phone in school.

Each member of staff, governor and volunteers is briefed and signs a "Code of Conduct" which includes using ICT safely and appropriately within school and outside of school. They are aware that it is their responsibility to remain professional / appropriate whilst using the Internet and other ICT in and out of school. This is outlined in the *Acceptable Use* policy.

Digital images and video

The school:

- Asks for parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs
- Staff sign the school's Acceptable Use of Technology Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work
- Pupils are taught that they should not post images or videos of others without their permission.