St Peter’s Church of England (VC) Primary School

Online Safety Policy

September 2022

# Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with ‘Keeping Children Safe in Education’ 2022 (KCSIE), ‘Teaching Online Safety in Schools’ 2019, statutory RSHE guidance 2019 and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside the school’s statutory Child Protection Policy. Any issues and concerns with online safety must always follow the school’s child protection procedures.

Online-safety risks are traditionally categorised as one of the 4 Cs: Content, Contact, Conduct or Commerce (see section 135 of KCSIE 2022). These areas provide a helpful approach to understand the risks and potential school response, whether technological or educational.

1. **Aims**

This policy aims to promote a whole school approach to online safety by:

* Setting out expectations for all St Peter’s C of E Primary School community members’ online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
* Helping safeguarding and senior leadership teams to have a better understanding and awareness of filtering and monitoring through effective collaboration and communication with technical colleagues
* Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
* Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today’s and tomorrow’s digital world, to survive and thrive online
* Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
  + for the protection and benefit of the children and young people in their care, and
  + for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
  + for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
* Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy.

Please see our Child Protection and Code of Conduct policies

# Roles and responsibilities

Ultimate responsibility for Online Safety rests with the headteacher and governing body. Whilst day to day duties can be delegated, this responsibility cannot.

## Governing body

The governing body must ensure that school has effective policies and procedures in place. As such, it will:

* Review this Online Safety policy at least annually and in response to any Online Safety incident. The review will consider:
  + whether the policy is up to date and covers all aspects of technology use within the school;
  + whether any Online Safety incidents were dealt with appropriately and following the framework in this policy; and
  + whether the policy was effective in managing any Online Safety incidents.
* Appoint one governor to have overall responsibility for the governance of Online Safety at school who will:
  + keep up to date with emerging risks and threats through technology use;
  + receive regular updates from the headteacher with regards to training, identified risks and any incidents; and
  + report to the Curriculum Committee as and when necessary.

## Headteacher/DSL

Reporting to the governing body, the headteacher has overall responsibility for Online Safety within school. The day to day management of this will be delegated to other staff and the Online Safety officer(s).

The headteacher will ensure that:

* Online Safety training for pupils, parents, staff and the governing body is planned, up to date and appropriate to the recipient.
* The designated Online Safety officers have had appropriate CPD in order to undertake the day to day duties.
* All Online Safety incidents are dealt with promptly and appropriately.

## Online Safety officer

The Online Safety officer(s) must:

* keep up to date with the latest risks to children whilst using technology, be familiar with the latest research and available resources for school and home use;
* recommend a programme of training and awareness for the school year to the headteacher and responsible governor for consideration and planning;
* review this policy regularly and bring any matters requiring update or amendment to the attention of the headteacher;
* advise the headteacher and governing body on all Online Safety matters;
* engage with parents and the school on Online Safety matters at school and at home;
* liaise with the local authority, IT technical support and other agencies as required;
* retain responsibility for the Online Safety incident log, ensuring staff know what to report and that there is an effective audit trail;
* ensure any technical Online Safety measures in school are fit for purpose through liaison with the local authority and/or IT technical support.
* be aware of any reporting function with technical Online Safety measures (for example the internet filter reporting function) and liaise with the headteacher and responsible governor to decide what reports are appropriate for viewing.

## ICT technical support staff

Technical support is provided to school by DK Huxter IT Services and Essex County Council.

Technical support staff are responsible for ensuring that:

* antivirus software is fit for purpose, up to date and applied to all capable devices;
* operating systems and devices are updated as appropriate;
* technical Online Safety solutions, such as internet filtering, are operating correctly;
* filtering levels are agreed with the Online Safety officer and headteacher and are applied appropriately (these may vary with the age of the user);
* filter logs are monitored on a regular basis in accordance with ECC best practice;
* standards are set for length, format and expiration of staff and pupils’ passwords, and passwords are applied correctly.

## All staff

Staff are responsible for ensuring that they:

* understand this policy and bring any queries to the headteacher for clarification;
* report any Online Safety incidents to the Online Safety officer and make an incident report if necessary;
* bring to the attention of the Online Safety officer or headteacher any inadequacies in their training.

PSHE/RSE Lead

* As listed in the ‘all staff’ section, plus:
* Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / RE / RSE curriculum, “complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds.”
* Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RE / RSE

## Pupils

Before using school ICT equipment, pupils must:

* have had teaching appropriate to their age and ability about the safe use of IT and what to do if something unexpected happens;
* understand and sign the acceptable use as agreed in the classroom.

Deviation from this policy or misuses of ICT equipment will be dealt with in accordance with school’s behaviour policy.

Children with SEN may require the information in the AUP to be provided in an alternative format, and school will ensure that all children receive the information in a format they are able to access.

## Parents

School will help parents and carers to have the skills and knowledge they need to ensure the safety of children. Parents should:

* take advantage of school-run Online Safety sessions and workshops;
* engage with their children in discussion about how Online Safety is managed in school;
* make use of resources provided by school via its website and newsletters.

# Education and curriculum

It is important that schools establish a carefully sequenced curriculum for online safety that builds on what pupils have already learned and identifies subject content that is appropriate for their stage of development.

As well as teaching about the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app, [Teaching Online Safety in Schools](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf) recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils.

RSHE guidance also recommends schools assess teaching to “identify where pupils need extra support or intervention [through] tests, written assignments or self evaluations, to capture progress.

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

* Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)
* Computing
* Citizenship

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place). “Parents and carers are likely to find it helpful to understand what systems schools use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online.”(KCSIE 2022)

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. disinformation, misinformation and fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

Annual reviews of curriculum plans (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

# Safe use

## Internet

Internet use will be granted to staff and pupils.

Staff should also refer to the Acceptable Use policy within the Staff Code of Conduct Policy

School filters all access to the internet. This means that access to inappropriate or illegal websites is prevented. Which websites are considered appropriate is decided and reviewed by the Online Safety officer, headteacher and IT support.

If filtering fails and an inappropriate site is accessed, this must be reported as an Online Safety incident (see below). It is essential that pupils know what to do (and what not to do) if something unexpected appears on their screen. This is covered in the AUP and must be reinforced during learning.

## Email

School’s email service should be used for professional work-related emails only. Emails of a personal nature are not permitted. Similarly, the use of personal email addresses for school business is not permitted.

All staff who need to send work-related emails have their own personal school email address.

All email is filtered and logged. Filtering should prevent any infected email from being sent from school or being received by school. This includes emails containing executable content (such as a virus) or spam. Although this and the antivirus protection in place on school equipment should offer sufficient protection from viruses contained within emails or attachments, it is sensible to consider carefully whether it is necessary to open an email or attachment from an unknown recipient and to pay attention to any warnings from the antivirus software.

The same standards are expected in emails as would apply when communicating on school letterhead or face to face. Communication must be courteous, accurate and appropriate spelling, grammar and punctuation must be used. Emails may form part of the records school or other bodies hold about pupils and it is good practice to assume that other professionals involved with the child may see them. Emails may also form part of information released under a freedom of information request or a Subject Access Request (SAR ).

Where it is necessary for staff to send information about pupils electronically, the content should be encrypted unless it is possible to anonymise the content successfully.

School equipment must not be used to access personal email.

The principles in this section should be applied to any inter-computer or electronic communication including web services, chat rooms, bulletin or news groups and text messaging.

## Photos and videos

School seeks permission from parents before making, using or publishing images of children. A copy of the form parents are asked to sign is appended to this policy.

School will never publish a child’s full name alongside an image of the child. Staff will only use school devices to make images of children, never their own. As soon as practicable after images are made, they will be transferred to an encrypted drive and deleted from the device on which they were made.

Images will be kept only for as long as they are useful to the school. Unwanted images will be deleted.

School continues to allow parents and pupils to photograph or record children on special occasions, and recognises that these photos or video will sometimes include images of other people’s children. While it is acceptable to share these images with friends and family, parents are reminded that particular vigilance is required if they are shared digitally. An image emailed or posted on a website is easily copied and disseminated and parents must be confident that those they allow to see the images will not share them more widely. This means, for example, that parents should not put photos on a Facebook page with no privacy settings, or in an unprotected tweet, unless those photos are already in the public domain or they have the permission of the parents/carers of all the children in the photos.

## Webcams and video conferencing

Webcams in school are used only for video conferencing and remote learning. This will always be supervised by a member of staff, and will take place only when school is satisfied that the video link is secure and can be seen only by the intended recipients. These will usually be in another school.

Only children whose parents have given permission will be involved in video conferencing.

Publically accessible webcams are not used in our school setting.

## Social networking

The Online Safety officer(s), headteacher and governor with responsibility for Online Safety will monitor and review the safety implications of school’s use of social networking sites. This is currently limited to Facebook

Policies relating to the publication of images of children will be relevant when engaging in social networking, and will be followed.

School discourages the engagement of staff with parents on social networking sites. We recognise, however, that, particularly in our small community, these relationships may exist and need not necessarily cause problems. Discussion of school business between staff and parents in a public forum is not appropriate, and we expect that all users of social networking will be responsible and aim to ensure that personal and professional reputations are not compromised by inappropriate postings. Activity by staff which undermines school’s reputation on social networking sites may lead to disciplinary action.

## Personal mobile devices (including phones)

School has a mobile phone for use by staff when off school premises. This may be used only for school purposes.

Staff should only use their personal mobile phones or devices at appropriate times of the day, for example break times. These must not be used to take photos or video of pupils. Personal mobile phones must never be used to make calls for school purposes.

Pupils should not bring mobile phones or devices into school. If there is a particular need for a child to bring a phone or device to school, it must be turned off and handed to the office to be kept in the safe until the child leaves for the day. If a pupil is found with a mobile device during the school day, it will be removed and his or her parents informed.

## Data

All school devices that hold personal data are encrypted. No data are to leave the school on an unencrypted device. Any loss of personal data is a serious Online Safety incident, over which the headteacher must liaise with the local authority. It is possible that such an incident will require reporting to the Information Commissioner’s Office since it may constitute a breach of the Data Protection Act 2018.

5. **Sexual Violence and Sexual Harassment**

DfE guidance on sexual violence and harassment has now been incorporated into Keeping Children Safe in Education and is no longer a document in its own right. It would be useful for all staff to be aware of this updated guidance: Part 5 covers the immediate response to a report, providing reassurance and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture and maintain an attitude of ‘it could happen here’. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as ‘low level’ are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

**Handling a sexting / nude and semi nude/ selfie incident:**

UKCCIS “Sexting in schools and colleges” should be used. This extract gives the initial actions that should be taken:

There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

* Whether there is an immediate risk to a young person or young people   
  *When assessing the risks the following should be considered:* 
  + Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
  + Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
  + Are there any adults involved in the sharing of imagery?
  + What is the impact on the pupils involved?
  + Do the pupils involved have additional vulnerabilities?
  + Does the young person understand consent?
  + Has the young person taken part in this kind of activity before?
* If a referral should be made to the police and/or children’s social care
* If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
* What further information is required to decide on the best response
* Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
* Whether immediate action should be taken to delete or remove images from devices or online services
* Any relevant facts about the young people involved which would influence risk assessment
* If there is a need to contact another school, college, setting or individual
* Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

An immediate referral to police and/or children’s social care should be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person’s developmental stage, or are violent
4. The imagery involves sexual acts and any pupil in the imagery is under 13
5. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply then a school may decide to respond to the incident without involving the police or children’s social care (a school can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children’s social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school’s pastoral support and disciplinary framework and if appropriate local network of support.

# Review and implementation

## Incidents

Any Online Safety incident must be brought to the attention of the Online Safety officer or, in his/her absence, the headteacher. The incident may be a breach of the security of data from a theft, a deliberate attack on the system, the unauthorised use of personal data by a member of staff, accidental loss or equipment failure. It might also be cyberbullying, the receipt by pupils of unsolicited emails or a failure of internet filtering resulting in inappropriate content being seen.

## Containment and recovery

Online Safety incidents always require an initial response to investigate and contain the situation, and if for example data have been lost, a recovery plan to ensure the continued successful operation of the school. The headteacher will decide who will lead on investigating the incident and ensure he or she has the appropriate resources.

The initial response will aim to clarify what happened and which children and staff were involved.

## Risk assessment

The risk assessment looks at the impact of what happened; are there adverse consequences for individuals or the school, how serious are these and how likely are they to occur?

## Notification

There are likely to be people who need to know if there has been a breach of Online Safety. These might include parents if pupils are involved, other staff members, the governing body and the local authority. The local authority will advise whether the Information Commissioner’s Office must be informed.

Informing people is not an end in itself. Notification should have a clear purpose; for example if a child has seen something inappropriate online, parents need to know how it happened and what steps are being taken to make sure it doesn’t happen again. This in turn helps them to reassure children that the upsetting incident should not reoccur.

## Evaluation and response

The incident log provides a record of the incident, how it was dealt with and what steps are in place to prevent reoccurrence. It will be filled in by the staff member involved. The log should be seen by the Online Safety officer, DSL, headteacher and responsible governor, who will consider whether this policy was helpful and sufficient and how it could be improved.

## Training

It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible. The Online Safety officer is responsible for being aware of new and emerging issues and drawing up an appropriate schedule of training and information giving for staff, pupils and parents. Pupils should find Online Safety embedded into the curriculum; wherever ICT is used in school staff will ensure that there are positive messages about the safe use of technology and risks.

An Online Safety incident might highlight the need for additional training or information, and the Online Safety officer will respond to this.

**St Peter’s C of E Primary School**

**Acceptable Use Agreement**

**How staff use school ICT**

School ICT equipment, including the intranet, should be used for school related purposes. Personal use is accepted on the provision usage is in accordance with this agreement, the e-safety policy and deemed reasonable by the deputy or headteacher.

When ICT equipment (other than issued laptops) is to be used off site, it is to be booked out using the equipment booking register found in the office.

When laptops are issued to individual staff, the user agreement must be signed. County guidance is that laptops are not to be left in cars unattended.

**Child safety**

It is our responsibility to educate and support our pupils to use electronic devices and the internet safely. We also have a responsibility to report to the Safeguarding Lead any e-safety issues which will be followed up and acted upon.

**Social Networking**

Social networking sites must not be accessed at school by staff unless for educational purposes where permission is granted by the deputy or headteacher e.g. Facebook account to report school sports, Tapestry. Seesaw to share children’s work. If social networking is to be used, age restrictions are to be upheld.

School related business is not to be discussed using social networking; this includes ‘private’ or ‘direct messaging’. As a member of the school community we have a responsibility for upholding the Code of Conduct, which states use of social networking must not adversely affect the reputation of the school or bring the school into disrepute.

Befriending of pupils and ex-pupils from our school on social networking sites is not to be accepted. Befriending of parents is not advised. Discussions of school related business or posting any comments or actions that could reflect on the school is not acceptable.

**Email**

All emails involving school business are to be sent and received using the allocated school email address. Only the office staff, deputy or headteacher can email parents directly.

**Audio, video and photography**

Audio, video and photographic files remain the property of the school at all times. These are to be stored on the school server or mobile devices (iPad, cameras). These types of files are to be used for school related business; they can be taken and used off site but you are responsible for safeguarding the files and minimising risks.

Only school equipment is to be used for recording audio, video or photographic files. Personal equipment is not to be used under any circumstances for recording these files – this is to safeguard you. You are able to use personal equipment to edit, manipulate and produce resources for these file types but you are responsible for safeguarding the files and minimising risks.

**File sharing**

File sharing, including the use of removable devices (memory sticks) and cloud based technologies is the responsibility of the user to safeguard the information being used and minimise risks. Mobile devices should not be used to transfer confidential information,

**Remote access**

You can remotely access the school network from any location but it is the responsibility of the user to safeguard the information being used and minimise risks. You must ensure that the device in which you are accessing the school network from is up to date with its latest anti-virus and malware software.

**Personal Devices**

* Personal devices such as mobile phones, tablet computers and laptops should not be used for personal use other than in staff areas e.g. staffroom or PPA room, during your own time. Personal tablets and laptops can be used for educational purposes at home but you must ensure that they are free from virus and malware which cannot be transferred to our school system. Please refer to the above section regarding audio, video and photography.

If you have any queries, are unsure of anything, or do not have a definitive answer for, please seek advice from ICT or the Headteacher before proceeding.

Any breaches of this agreement could lead to disciplinary action under the school’s disciplinary procedure, including dismissal in serious cases.

I confirm that I have read and understood the above.

Signed ………………………………………………………. Date ………………..

Acceptable use policy for pupils

I promise that when I am trusted to use school computers and ipads I will be sensible and responsible.

I promise not to look for or show other people things that may be upsetting.

I promise to show respect for the work other people have done.

I will not use other people’s work or pictures without permission.

I will not damage the ICT equipment and if I accidentally damage something I will tell my teacher.

I will not tell anybody my password. If I forget my password I will tell my teacher.

I will not use other people’s usernames or passwords.

I will not download anything from the internet unless my teacher has asked me to.

I will tell my teacher if anybody asks me for personal information.

I will tell my teacher if anybody says or does anything to me that is hurtful or upsets me.

I will turn off my screen and tell a teacher if I see something upsetting.

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 that some people can be nasty. I will tell my teacher or my parents if I am worried.

I understand that if I break these rules there will be consequences and my parents will be told.

**Name:**

**Signature (child):**

**Signature (parent):**

**Date:**Photo permissions form for pupils

Occasionally, we may take photographs of the pupils at our school. We may use these images in printed publications that we produce, as well as on our website or on project display boards at our school. We may also make video or webcam recordings for school-to-school conferences, monitoring or other educational use.

Essex County Council may also use our photographs of pupils to illustrate work in Essex schools in council publications, publicity materials and the internet.

From time to time, our school may be visited by the media who will take photographs, film footage or carry out radio interviews. Pupils will often appear in these images, which may appear in local or national newspapers, or on televised news programmes. Photos for the media and other publicity purposes may also be taken at events where our school is taking part.

Please answer the question below, then sign and date the form where shown. Please return the completed form to the school.

|  |  |
| --- | --- |
| 1. Are you happy for your child’s photograph /video to be taken when participating in school activities? This may include photos and videos by other parents at school plays and events.   Use may include:  Hard copy publications and publicity materials produced by the school and by Essex County Council  The school website, school social media and Essex County Council website and social media   Use by educational establishments and providers with which school is working (eg Children's University videos on YouTube)  Any other educational activity the school undertaken by the school | YES/NO |

Name of Child: ………………………………………………………………………………………………………………

Parent/Carer Signature: ……………………………………………………………… Date: ………………….

Parent/Carer Name Printed: ……………………………………………………………………………………….