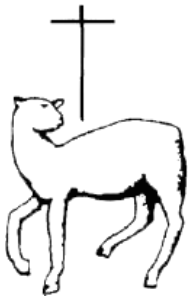
St John's C of E VA First School

ONLINE SAFETY POLICY



'Together we have roots to grow and the wings to fly.'

This policy should be taken as part of St. John's C. of E. First School's overall strategy and is implemented within the context of our vision of Government aims and our values as a Church of England School.

Review

Review Cycle	Date of Current Policy	Author(s) of Current Policy	Review Date
	25.09.2023	Teresa Gilbert	

Ratification

Role	Name	Signature	Date
Chair of Governors	**Claire Levene Plumb**	**CLAIRE LEVENE PLUMB**	
Head Teacher	**Teresa Gilbert**	**TERESA GILBERT**	
DSL	**Teresa Gilbert**	**TERESA GILBERT**	

Details of Policy Updates

Date	Details

Roles and responsibilities

The Head teacher and Governors oversee the safe use of technology when children and learners are in their care and act immediately if they are concerned about bullying, radicalisation or other aspects of children's well-being. They are responsible for ensuring the safety (including online and the prevention of being drawn into terrorism) of all members of the school community. They have concern for the online reputation of the school.

The Online Safety Leader will work with the Head teacher and the Designated Safeguarding Lead (DSL), to have an overview of the serious child protection issues that arise from sharing of personal data, access to illegal or inappropriate materials (including extremism and radicalisation, inappropriate online contact with adults, potential or actual incidents of grooming and cyber-bullying).

An Online Safety working group will work with the Online Safety Leader to implement and monitor the Online Safety Policy and Acceptable User Policies (AUP). This group is made up of Online Safety Leader, Designated Safeguarding Lead (DSL), teacher, governor, member of support staff, technician, member of senior leadership team and pupils. Pupils are an important part of this group, working with them through the School Council, to contribute their knowledge and use of technology. They meet on a termly basis.

Role	Responsibility
Governors	Monitor the effectiveness of the Online Safety Policy Delegate a governor to act as Online Safety link Online Safety Governor works with the Online Safety Leader to carry out regular monitoring and report to Governors Verify that the filtering, monitoring and or supervision systems are in place to identify children accessing or trying to access harmful and inappropriate content online
Head Teacher and Senior Leaders	Ensure that all staff receive suitable Continuing Professional Development (CPD) to carry out their Online Safety roles including online risks of extremism and radicalisation Create a culture where staff and learners feel able to report incidents Ensure that there is a progressive Online Safety curriculum in place Ensure that there is a system in place for monitoring Online Safety Follow correct procedure in the event of a serious Online Safety allegation being made against a member of staff or pupil Inform the local authority about any serious Online Safety issues Ensure that the school infrastructure/network is as safe and secure as possible Ensure that policies and procedures approved within this policy are implemented Use an audit[1] to annually review Online Safety with the school's technical support
Online Safety Coordinator	Lead the Online Safety working group Coordinate work with the school's Designated Safeguarding Lead (DSL)

[1] https://staffonly.somerset.org.uk/sites/edtech/Subscriber%20Only/Questions%20for%20Technical%20Support%20v4.pdf

	Log, manage and inform others of Online Safety incidents and how they have been resolved where this is appropriate Lead the establishment and review of Online Safety policies and documents Lead and monitor a progressive Online Safety curriculum for pupils Ensure all staff are aware of the procedures outlined in policies relating to Online Safety Provide and/or broker training and advice for staff Attend updates, subscribe to appropriate newsletters and liaise with the LA Online Safety staff and technical staff Meet with Senior Leadership Team and Online Safety Governor to regularly discuss incidents and developments
Teaching and Support Staff	Participate in any training and awareness raising sessions Read, understand, sign and act in accordance with the AUP and Online Safety Policy Report any suspected misuse or concerns to the Online Safety Leader / Designated Safeguarding Lead (DSL) and check this has been recorded Provide appropriate Online Safety learning opportunities as part of a progressive Online Safety curriculum Model the safe, positive and purposeful use of technology Monitor the use of technology in lessons, extracurricular and extended school activities Demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks, making sure that these are in line with school ethos and policies, including at the time of a Critical Incident
Pupils	Read, understand, sign and act in accordance with the Pupil AUP / agreed class internet rules Report concerns for themselves or others Make informed and positive choices when using technology in school and outside school, considering the effect on themselves and others
Parents and Carers	Endorse (by signature) the Pupil AUP Discuss Online Safety issues with their child(ren) and monitor their home use of technology (including tablets, mobile phones and games devices) and the internet Keep up to date with issues through newsletters and other opportunities Inform teacher / Headteacher of any Online Safety concerns Use formal channels to raise matters of concern about their child(ren)'s education

	Maintain responsible standards when referring to the school on social media
Technical Support Provider	Ensure the school's ICT infrastructure is as secure as possible and is protected from misuse or malicious attack Ensure users may only access the school network using an approved password Maintain and inform the Senior Leadership Team of issues relating to filtering Keep up to date with Online Safety technical information and update others as relevant Ensure use of the network is regularly monitored in order that any misuse can be reported to the Online Safety Leader for investigation Ensure monitoring systems are implemented and updated Ensure all security updates are applied (including anti-virus and Windows) Sign an extension to the Staff AUP detailing their extra responsibilities
Community Users	Sign and follow the Guest/Staff AUP before being provided with access to school systems Demonstrate appropriate standards of personal and professional conduct in line with the AUP

Education of pupils

'Children are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum.'

Keeping Children Safe 2023

A progressive planned Online Safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited. Breadth and progression is ensured through reference to UKCCIS Education for a Connected World framework[2] and is implemented through the use of Somerset ActiveBYTES scheme[3].

Within this:

- key Online Safety messages are reinforced through Collective Worship presentations, Safer Internet Week (February), Anti-bullying Week (November) and throughout all teaching
- pupils are taught to keep themselves safe online and to be responsible in their use of different technologies as detailed in the Somerset ActiveBYTES scheme of work
- pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material

- in lessons where internet use is pre-planned and where it is reasonable, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches

[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/680356/Education_for_a_Connected_World2.pdf
[3] https://staffonly.somerset.org.uk/sites/edtech/SitePages/e-Safety/ActiveBYTES.aspx

- pupils are taught to be critically aware of the content they access online, including recognition of bias and extreme or commercial content. They are guided to validate the accuracy and reliability of information
- pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- the Online Safety Coordinator maintains and passes on knowledge of current concerns to be included within learning experiences
- pupils are provided with opportunities to influence the online safety curriculum
- pupils will write and sign an AUP at the beginning of each school year, which will be shared with parents and carers
- pupils are educated to recognise and respond appropriately to 'different forms of
- bullying, including cyber-bullying' and given opportunities to support each other

Education and information for parents and carers

Parents and carers will be informed about the ways the internet and technology is used in school. They have a critical role to play in supporting their children with managing Online Safety risks at home, reinforcing key messages about Online Safety and regulating their home experiences. The school supports parents and carers to do this by:

- providing clear AUP guidance which they are asked to sign with their children
- providing regular newsletter items in the St John's Journal and appropriate support materials
- raising awareness through activities planned by pupils
- inviting parents to attend activities such as Online Safety week, Online Safety
- Collective Worship presentations or other meetings as appropriate
- providing and maintaining links to up to date information on the school website

Training of Staff and Governors

There is a planned programme of Online Safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the AUPs. This includes:

- all staff knowing the Designated Safeguarding Lead and the Online Safety Lead and their responsibilities
- an annual audit of the Online Safety training needs of **all** staff
- **all** new staff and governors receiving Online Safety training as part of their induction programme through Safeguarding training. Online safety training provided every two years.
- providing information to supply and student teachers on the school's Online Safety procedures
- the Online Safety Leader receiving regular updates through attendance at training sessions and by reviewing regular Online Safety newsletters from the LA
- this Online Safety Policy and its updates being shared and discussed in staff meetings and in Governor meetings
- the Online Safety Leader providing training within safeguarding training and as specific online safety updates and reviews
- the Online Safety Leader providing guidance as required to individuals and seeking LA support on issues
- *staff and governors are made aware of the Professionals Online Safety Helpline (POSH) 0344 381 4772*

Online bullying

Online bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

The school will follow procedures in place to support anyone in the school community affected by online bullying.

Pupils and staff are made aware of a range of ways of reporting concerns about online bullying. This may be by; telling a trusted adult, Online bully box, Childline App and phone number 0800 1111, POSH helpline 0344 381 4772.

Pupils, staff and parents and carers are informed of their responsibilities to report any incidents of online bullying and advised to keep electronic evidence.

All incidents of online bullying reported to the school will be recorded by the school in the behaviour log and safeguarding portal My Concern.

The school will follow procedures to investigate incidents or allegations of online bullying.

The school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.

Pupils, staff and parents and carers will be required to work with the school to support the approach to online bullying and the school's Online Safety ethos.

Sanctions for those involved in online bullying will follow those for other bullying incidents as indicated in the schools Behaviour Policy or AUP and may include:

- the bully being asked to remove any material deemed to be inappropriate or the service provider being contacted to remove content if the bully refuses or is unable to delete content
- internet access being suspended at the school for a period of time.
- the parent and carers of pupils being informed
- the police being contacted if a criminal offence is suspected

Sexting

The school will provide appropriate support for sexting incidents which take place in and out of school. Within school, any device which has an illegal image of a child under 18, or is suspected of having such an image, will be secured and switched off. This will then be reported to the Designated Safeguarding Lead (DSL). An individual member of staff will not investigate, delete or pass on the image. The Designated Safeguarding Lead (DSL) will record any incident of sexting and the actions taken in line with advice from Somerset Local Authority.

Prevent

The school works to ensure children are safe from terrorist and extremist material when accessing the internet on the premises. Appropriate levels of filtering are in place through a managed filtering service which includes terms related to terrorism. Appropriate monitoring of internet use will identify attempts to access such material. Children are educated to evaluate information accessed with a reporting procedure that identifies inappropriate sites so that action, including blocking, can be put into place.

Technical Infrastructure

The person(s) responsible for the school's technical support and those with administrator access to systems will sign a technician's AUP, in addition to the staff AUP.

The school ensures, when working with our technical support provider that the following guidelines are adhered to:

- the School ICT systems are managed in ways that ensure that the school meets Online Safety technical requirements
- there are regular reviews and audits of the safety and security of school ICT systems.
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations and other devices from accidental or malicious attempts which might threaten the security of the school systems and data with regard to:

- ensuring ongoing backups take place and, in case of an incident, the school can restore data in line with our business continuity plan
- the downloading of executable files by users
- the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices used out of school
- the installing of programs on school devices unless permission is given by the technical support provider or Computing/ICT coordinator
- the use of removable media (e.g. memory sticks) by users on school devices. (see School Personal Data Policy for further detail)
- the installation of up to date anti-virus software

- access to the school network and internet will be controlled with regard to:
  - users having clearly defined access rights to school ICT systems through group policies
  - users being provided with an appropriate username and password (considering accessibility of users with particular needs where supervision is put in place to monitor activity)
  - staff users being made aware that they are responsible for the security of their username and password which they are required to change every 60 days; they must not allow other users to access the systems using their log on details
  - the 'master/administrator' passwords are available to the Headteacher and kept in the school safe
  - users must immediately report any suspicion or evidence that there has been a breach of security
  - an agreed process being in place for the provision of temporary access of "guests" (e.g. trainee or supply teachers, visitors) onto the school system. Anyone allowed unsupervised access must sign the staff AUP and be made aware of this Online Safety Policy
- the internet feed will be controlled with regard to:
  - the school's responsibility[4] to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system" Keeping Children Safe 2022
  - Foundation Stage and Key Stage 1 pupils' access will be supervised with
  - access to specific and approved online materials
  - Key Stage 2 pupils' will be supervised. Pupils will use age-appropriate search engines and online tools and activities
  - requests from staff for sites to be removed from the filtered list being approved by the Senior Leadership Team and logged[5]
  - user based filtering used to provide differentiated access for staff and pupils
  - filtering issues being reported immediately
- the IT System of the school will be monitored with regard to:
  - the school IT technical support regularly monitoring and recording the activity of users on the school IT systems
  - Online Safety incidents being documented and reported immediately to the Online Safety Leader or Designated Safeguarding Lead (DSL) who will arrange for these to be dealt with immediately in accordance with school policies

Data Protection

The school's Data Protection Policy provides full details of the requirements that are met in relation to Data Protection regulations.

The school will:

- at all times take care to ensure the safe keeping of personal and sensitive data, minimising the risk of its loss or misuse which must include regular back-ups and anti-virus protection updates

[4] https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

[5] https://staffonly.somerset.org.uk/sites/edtech/eSafety/Filter/Benefit%20Analysis%20request%20for%20unfiltering%20a%20website.pdf

- use personal data only on secure password protected computers and other devices
- ensure that users are properly 'logged-off' at the end of any session in which they are accessing personal data
- provide staff with secure equipment/services to store or transfer data eg remote
- access, encryption and secure password protected devices
- remove data in line with the school's Data Retention Policy
- ensure that all staff are aware of the need to immediately report any loss of personal or sensitive data to the Data Protection Lead
- complete a privacy impact assessment and check the terms and conditions of sites/apps used for learning purposes to ensure that any pupil personal data is being held securely

Use of digital images and sound

Photographs, video and sound recorded within school are used to support learning experiences across the curriculum, to share learning with parents and carers on our school's learning platform and to provide information about the school on the website. The school will:

- build a culture where permission is always sought before a photo is taken or video and sound are recorded; including encouraging pupils to seek permission from other pupils to take, use, share, publish or distribute images and sound
- ensure verifiable permission[6] from parents or carers is obtained before images, sound recordings or videos of pupils are electronically published on the school website, on social media or in the local press. The written consent, where pupils' images, video and sound are used for publicity purposes, is kept until the data is no longer in use
- when using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites
- allow staff to take images, record video and sound to support educational aims, following the school policy regarding the sharing, distribution and publication of those. School equipment only is used. Personal equipment of staff is not allowed for this purpose (See Mobile Phone Policy)
- make sure that images, sound or videos that include pupils will be selected carefully with their knowledge, taking care when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- make adults and children aware of the risk that any published image, video and sound could be harvested, reused and repurposed
- ensure that pupils' full names will not be used anywhere on the school website, school blogs or within school branded social media, particularly in association with photographs
- not publish pupils' work without their permission and the permission of their parents or carers
- only hold digital/video images on school approved secure storage areas. There is an expectation that images and recordings are not retained longer than necessary and in line with the schools Data Retention Policy
- in accordance with guidance from the Information Commissioner's Office, parents/carers can take videos and digital images or sound recordings of their children at school events for their own personal use. It is made clear that, to respect everyone's privacy and in some cases protection, these are not to be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images or in the sound recording. We ask parents/carers not to take digital/video images or record sound during an event if it is felt that it would spoil the experience for others. A statement is made before an event as to the expectations of the school
- make clear to professional photographers who are engaged to record any events or provide a service that they must work according to the terms of the settings Online Safety Policy and will sign an agreement which ensures compliance with the Data Protection regulations and that images will only be used for a specific

[6] https://staffonly.somerset.org.uk/sites/edtech/eSafety/Policies/Pupil_images_consent%20form.doc

purpose, subject to parental consent. Photographers will not have unsupervised access to children and young people

Communication (including use of Mobile Devices and Social Media)

A wide range of communications technologies increases effective administration and has the potential to enhance learning. St John's First school will:

- with respect to email
  - ensure that the school uses a secure business email system for communication
  - ensure that personal information is not sent via unsecure email
  - ensure that governors use a secure email system
  - ensure that any digital communication between staff and pupils or parents and carers is professional in tone and content
  - make users aware that email communications will be monitored by the school
  - inform users what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature
  - teach pupils about email and other communication tools alongside online safety issues through the scheme of work and implementation of the AUP
  - only publish official staff email addresses where this is required
  - protect the identities of multiple recipients by using bcc in emails
- with respect to social media e.g. YouTube, Facebook, Twitter, blogging and personal publishing
  - enable online learning opportunities to make use of age appropriate educationally focussed sites that will be moderated by the school
  - control access to social media and social networking sites in school
  - provide staff with the tools to risk assess sites before use and check the sites terms and conditions to ensure a) the site is age appropriate b) whether content can be shared by the site or others without additional consent being given
  - ensure that any digital communication between staff and pupils or parents and carers is open, transparent and professional in tone and content
  - discuss with staff the personal use of email, social networking, social media and personal publishing sites as part of staff induction, building an understanding of safe and professional behaviour in line with DfE advice[7], being careful about subjects discussed online
  - staff are advised that no reference should be made to pupils, parents/carers or school staff on their personal social networking accounts
  - register concerns (e.g. recording in Online Safety log) regarding pupils'
  - inappropriate use of email, social networking, social media and personal publishing sites (in or out of school) and raise with their parents and carers, particularly when concerning pupils' underage use of sites
  - support staff to deal with the consequences of hurtful or defamatory posts about them online
  - inform the staff that in the case of a **Critical Incident** they should not make any comment on social media without the permission of the senior management team
- with respect to personal devices (including consideration of Keeping Children Safe 20188)
  - inform staff that personal devices should only be used at break and lunchtimes in restricted areas when they are not in contact with pupils, unless they have the permission of the Headteacher (turned off at other times)
  - ensure that staff understand that the AUP will apply to the use of their own portable / wearable device for school purposes

[7] DfE Cyberbullying Advice for headteachers https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf and Teaching Standards 2012 https://www.gov.uk/government/publications/teachers-standards

[8] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/707761/Keeping_Children_Safe_in_Education_-_September_2018.pdf page 93

- inform staff and visitors that they are not allowed to use personal devices to take photographs or video in school for any purpose without the express permission of SLT
- check any use of a personal device for an education purpose (where permission has been given) only uses the school's internet connection on the school site
- remind all that personal devices should be pin code or fingerprint protected and not discoverable by third parties
- advise staff not to use their personal mobile phone to contact pupils, parents and carers
- provide a mobile phone for activities that require them
- challenge staff and visitors when there is suspected misuse of mobile phones or devices