ST JOHN'S CHURCH OF ENGLAND PRIMARY SCHOOL

ONLINE SAFETY POLICY

ACCEPTABLE USE POLICY

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-

bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Roles and responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governor who oversees online safety is Cath Ascroft.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.

The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead

Details of our school's DSL are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

The Online Safety Officer

The Online Safety Officer is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL and Online Safety Officer to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Adhere to our Acceptable Use policy – available on our school website or paper copies can be requested from the school office.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study.

From September 2020 **all** schools will have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

This new requirement includes aspects about online safety. As such these expectations are outlined in italics below.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

*By the **end of primary school**, pupils will know:*

- *That people sometimes behave differently online, including by pretending to be someone they are not.*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*
- *How information and data is shared and used online*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to adhere to our Acceptable Use policy. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Pupils using mobile devices in school

Pupils are allowed, but not encouraged, to bring mobile devices into school if their parents/carers deem it necessary. Mobile devices, including phones and tablets, are not permitted to be used during school hours. Devices will be signed in and out each day and kept locked in the school office.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.

Work devices must be used solely for work activities.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Monitoring arrangements

The DSL and Online Safety Officer logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed annually by the Online Safety Officer. At every review, the policy will be shared with the governing board.

Approved by: C. Ascroft (Governing body) and P. Thomson (headtacher)

Last reviewed: September 2021

Next review due: September 2022

St John's Church of England Primary School

Acceptable Use Agreement (staff, governors, volunteers and visitors)

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without prior parental/carer consent.
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

- I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.
- I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- I will let the designated safeguarding lead (DSL) and Online Safety Officer know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

St John's Church of England Primary School

Acceptable Use Agreement (parents and carers)

New technologies have become integral to the lives of children and young people in today's society, both within and outside school. The internet, digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

At St. John's Church of England Primary School, we want to ensure:

- young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- school ICT systems and users are protected from accidental or deliberate misuse which could put the security of the systems and users at risk.
- parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

Parents/carers are kindly requested to read and adhere to our Acceptable Use Policy. If you would like to request a paper copy, please contact the school office. Further online safety information is available on our school website or please speak to our Online Safety Officer (Miss G Lovelock).

- As the parent/carer of a pupil(s) at St John's Church of England Primary School, I give permission for my son/daughter to have access to the internet and to ICT systems at school.
- I know that my child has read their own ICT Pupil Rules and will receive online safety education to help them understand the importance of the safe use of ICT, both in and out of school.
- I understand the school will take every reasonable precaution, including monitoring and filtering systems, to ensure pupils will be safe when they use internet and ICT systems.
- I recognise that school cannot ultimately be held responsible for the nature and content of materials accessed on the internet.
- I understand that if my child does not follow these online safety rules, they could be stopped from using the computers in school.
- I am aware that my child's activity on ICT systems will be monitored and I will be contacted if there are any E-safety concerns.
- I will encourage my child to adopt safe use of internet and digital technologies at home and will inform school if I have concerns over my child's online safety.

Addendum to Online Safety Policy March 2020

Response to COVID-19

In response to the COVID-19 pandemic, the UK Government has issued guidance and advice about coronavirus in educational settings for staff, parents and carers, pupils and students. Coronavirus (COVID-19): safeguarding in schools, colleges and other providers, published by the Department for Education (March 2020), refers to the necessity for safeguarding procedures for remote learning.

There have been significant changes within our setting in response to the outbreak. The majority of pupils are now at home and staffing is likely to be significantly affected through illness and self-isolation. Despite the changes, the school's Child Protection Policy is fundamentally the same: children and young people always come first, staff should respond robustly to safeguarding concerns and contact the DSL in line with our established safeguarding procedure.

At St John's Church of England Primary School, we already have robust safeguarding procedures currently in place. Our Child Protection Policy and Online Safety Policy are available on the school website or a paper copy is available from the school office upon request. This addendum sets out some of the adjustments we are making in line with the changed arrangements in the school and following advice from government and local agencies.

Please note this guidance refers to **remote learning** only.

Risk online

Pupils will be using the internet more during this period. We are using our school website, managed by School Spider, to provide home learning activities. Staff will be aware of the signs and signals of cyberbullying and other online risks and apply the same child-centred safeguarding practices as when children were learning at school.

- We are continuing to ensure appropriate filters and monitors are in place for the children of key workers/vulnerable children still in school. We will liaise with our technical support for as long as we are able under the unprecedented circumstances.
- Our school website is managed by School Spider, which is GDPR-compliant.
- We have taken on board guidance from the UK Safer Internet Centre on safe remote learning. We have reviewed the code of conduct and information sharing policy accordingly - information will only be shared with school staff as necessary for the setting of work.
- Staff have been reminded of the school's code of conduct and importance of using school systems to communicate with children and their families.
- Children accessing remote learning receive guidance on keeping safe online and know how to raise concerns with the school, Childline, the UK Safer Internet Centre and CEOP. Links are available to parents and pupils through our school website.

- At present, it is worth noting that we will not be delivering live lessons in order to help safeguard pupils and staff.
- Parents and carers have received information about keeping children safe online with peers, the school, other education offers they may access and the wider internet community. We have set out the school's approach, including the sites children will be asked to access and set out who from the school (if anyone) their child is going to be interacting with online. Parents have been offered the following links:

    - Internet matters - for support for parents and carers to keep their children safe online
    - London Grid for Learning - for support for parents and carers to keep their children safe online
    - Net-aware - for support for parents and carers from the NSPCC
    - Parent info - for support for parents and carers to keep their children safe online
    - Thinkuknow - for advice from the National Crime Agency to stay safe online
    - UK Safer Internet Centre - advice for parents and carers

Staff Expectations

Staff should continue to look out for signs that a child is at risk while they're not at school, including when interacting with them online. They should follow policy for reporting concerns, and make referrals to children's social care and the police as needed.

Staff are also required to adhere to our Acceptable Use Policy when using the internet at school or home.

Parent/Carer Expectations

Most of our remote learning resources are accessible through our school website. Parents/carers are asked to contact the school directly if they do not have the ability to access these resources for their child(ren). Parents/carers are invited to use our enquiries email should they wish to contact us or to share any learning from their child to be celebrated on the school website.

We kindly request parents/carers to adhere to our Acceptable Use Policy for Parents and Carers, available on the school website.

We recommend parents supervise their children whilst they are using devices with internet access. Whilst the resources made available on our Home Learning page via the school website are all free and from reputable organisations/sources, there is always a risk of children accessing external links which are not recognised by our school. We urge parents/carers to remind children of the risks.

Last reviewed: November 2021

Next review due: September 2022