St. John's Angell Town C of E Primary School

Online Safety Policy

Reviewed	**Autumn 2024**
Next Review	**Autumn 2029**

Vision

Learning to make the world a better place through Faith, Hope and Love

'Three things will last forever – faith, hope and love – and the greatest of these is love.'

1 Corinthians 13:13

Vision Statement

Learning to make the world a better place through, faith, hope and love.

We value all children as unique and welcome them into our safe, loving and supportive St John's family. We nurture children to flourish and aspire to reach their God given potential. We rejoice in our rich diversity and our broad, balanced curriculum provides opportunities for all to achieve excellence, open minds and inspire dreams both now and the future.

Faith

Faith gives us confidence, the resilience to challenge ourselves and achieve more.

'Faith can move mountains' Matthew 17:20

Hope

Hope gives us aspirations for our future; to do our best and support each other.

'But those who hope in the Lord will renew their strength. They will soar on wings like eagles' Isiah 40:31

Love

We should Love one another, respect each other and work together.

'Love is more important than anything else. It's what ties everything completely together.' Colossian's 3:14

This is our Christian foundation which enables us to encourage and inspire one another so that we may all thrive in a safe and nurturing environment.

We value all children as unique and welcome them into our safe, loving and supportive St John's family. We nurture children to flourish and aspire to reach their God given potential. We rejoice in our rich diversity and our broad, balanced curriculum provides opportunities for all to achieve excellence, open minds and inspire dreams both now and the future.

St John's Angell Town C of E Primary School provides a happy, secure and stimulating learning environment where Christian values are embraced by all. We offer excellent pastoral care to our children, and our creative curriculum coupled with our strong sense of community ensures that we are a happy, forward-thinking and successful school.

Our mission statement says that we aim to achieve this through:

- ✓ Reflecting the teachings of Jesus Christ in our daily lives
- ✓ Providing a warm and welcoming environment for our school and thewider community
- ✓ Fostering a lasting love of learning
- ✓ Encouraging and celebrating achievement
- ✓ Expecting the highest standards of work and behaviour
- ✓ Effective teaching which develop independence and inspires creativity ina broad and balanced curriculum
- ✓ Addressing individual needs and diversity within an inclusive ethos.

Our Curriculum Drivers:

Our overarching school aims are shaped by our Curriculum Drivers. The drivers are the core teaching and learning principles that we value as a school.

We use our Curriculum Drivers as guiding principles ensuring that we offer a curriculum that is rich in its skills and knowledge base, is personalised and is geared to meet the interests and ambitions of our learners.

At St John's School we have the following Curriculum Drivers:

- Cultural Capital
- Knowledge Driven
- Language and Communication
- Faith, Hope and Love (Spirituality)
- Collectively our Curriculum Drivers help to foster high aspiration in our learners. This is the golden thread that knits all of the drivers together.

Our Curriculum Drivers work in tandem with the vision and values of the school.

Curriculum Drivers (st-johns.lambeth.sch.uk)

Curriculum Drivers v4.pptx - Google Slides

AI Use to Support Learning –

Artificial Intelligence (AI) tools may be used within the curriculum to enhance learning, creativity, and productivity. Students and staff are encouraged to use AI thoughtfully as a support for idea generation, research, drafting, and problem-solving. AI must be used in ways that uphold academic integrity: AI should assist learning, not replace it. Work submitted for assessment must represent the learner's own understanding, with any AI-generated contributions clearly acknowledged where appropriate.

AI use must also meet the school's safeguarding and online safety expectations. Staff will ensure that students use age-appropriate tools, understand risks such as misinformation, bias, and unsafe content, and know how to report concerns. AI tools should only be used within approved platforms that meet data-protection and child-safety requirements.

Schemes of learning must be followed with fidelity, ensuring that AI is used to strengthen planned teaching rather than replace curriculum intent. Teachers will integrate AI only where it supports the learning objectives, maintains challenge, and preserves the development of core knowledge and skills. AI should not be used to bypass essential learning experiences or reduce opportunities for critical thinking.

Staff will guide students in developing the digital literacy, critical thinking, and ethical awareness needed to use AI safely, responsibly, and effectively.

St John's Angell Town Primary School

ONLINE SAFETY POLICY

1. Aims

St John's Angell Town Primary School is committed to ensuring that pupils, staff, volunteers and governors can use digital technologies safely, confidently and responsibly. Our aims are to:

- Maintain robust processes to ensure online safety for the whole school community.
- Deliver an effective whole-school approach that empowers pupils and adults to use technology safely, including mobile and smart devices.
- Establish clear mechanisms to identify, intervene, record and escalate online safety concerns.
- Ensure our practice aligns with Keeping Children Safe in Education (KCSIE) 2024–2026, the Online Safety Act 2023–2025, and DfE Filtering & Monitoring Standards (2023–2026).

1.2 Categories of Online Risk

We follow the DfE's four-risk model ():

- Content – exposure to harmful or illegal content (pornography, extremism, hate content, self-harm, misinformation, deepfakes).
- Contact – harmful interactions (grooming, coercion, impersonation, radicalisation, commercial exploitation).
- Conduct – harmful behaviour (bullying, sharing nudes/semi-nudes, harassment, reputation damage).
- Commerce – financial risks (scams, phishing, gambling, fraudulent transactions).

2. Legislation and Guidance

This policy complies with:

- *Keeping Children Safe in Education (KCSIE) 2024–2026*
- *Online Safety Act 2023–2025*
- *DfE Filtering & Monitoring Standards (2023–2026)*
- *Prevent Duty Guidance (2024–2026)*
- *UKCIS Sharing Nudes & Semi-Nudes (2023–2026)*
- *Education Act 1996, 2006, 2011* (including powers to search/delete data on pupil devices) ()
- *Equality Act 2010*
- *NCSC Cyber Security Standards for Schools (2024–2026)*

It also reflects the National Curriculum for Computing and statutory RSE/Health Education requirements.

3. Roles and Responsibilities

3.1 Governing Body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account (). Governors ensure:

- Compliance with DfE filtering and monitoring standards.
- Annual review of filtering and monitoring effectiveness.
- Staff receive annual online safety training and regular updates.
- Online safety is embedded across safeguarding, curriculum and behaviour policies.
- Provision is adapted for vulnerable pupils and those with SEND.
- Termly oversight of online safety logs and DSL reports.

3.2 Headteacher (Strategic Lead)

The headteacher is responsible for:

- Ensuring staff understand and consistently implement this policy ().
- Overseeing the DSL and ICT Lead in relation to filtering, monitoring, incident management and staff training.
- Ensuring online safety is embedded across all school systems.
- Ensuring online safety risks are included in whole-school safeguarding and risk assessments.
- Reporting significant online safety issues to governors.

3.3 Designated Safeguarding Lead (Operational Lead)

The DSL takes lead responsibility for online safety (), including:

- Managing filtering and monitoring systems.
- Logging, analysing and escalating online safety incidents.
- Ensuring incidents involving nudes/semi-nudes follow UKCIS guidance.
- Responding to concerns involving AI-generated content or deepfakes.
- Delivering annual online safety training and updates.
- Liaising with external agencies (police, social care, Prevent, IT providers).
- Conducting annual online safety risk assessments.
- Providing termly online safety reports to the headteacher and governors.

3.4 Deputy DSLs

Deputy DSLs support the DSL and must be trained to the same standard.

3.5 ICT Lead / E-Safety Coordinator

The ICT Lead is responsible for ():Maintaining secure systems aligned with NCSC standards.

- Conducting monthly security checks.
- Updating filtering and monitoring systems.
- Blocking harmful content and preventing unsafe downloads.
- Supporting staff with technical aspects of online safety.

3.6 Staff and Volunteers

All staff must ():

- Follow acceptable use agreements.
- Report concerns immediately to the DSL.
- Support pupils to recognise and report risks.
- Maintain an attitude of *"it could happen here."*
- Respond appropriately to online sexual harassment or violence.

3.7 Parents and Carers

Parents are expected to ():

- Support acceptable use expectations.
- Raise concerns with staff or the DSL.
- Engage with school-provided online safety guidance.

3.8 Visitors and Community Users

Visitors using school ICT systems must follow the acceptable use agreement ().

4. Educating Pupils About Online Safety

Online safety is taught through:

- Computing curriculum
- RSE and Health Education
- PSHE
- Cross-curricular opportunities

Key Stage 1

Pupils learn to ():

- Use technology safely and respectfully.
- Keep personal information private.
- Seek help when concerned.Key Stage 2

Pupils learn to ():

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Report concerns about content or contact.

By the end of primary school, pupils will understand ():

- Online identity, impersonation and anonymity.
- Respectful online behaviour and digital boundaries.
- Risks of harmful content and contact.
- How to critically evaluate online information.

- How AI-generated content can mislead or manipulate.
- How data is shared and used online.
- How to respond safely to unknown adults online.

Teaching is adapted for vulnerable pupils and those with SEND ().

5. Educating Parents

The school raises parent awareness through:

- Letters and communications home ()
- Website and VLE information
- Parents' evenings
- Online safety guidance from trusted organisations

Parents should raise concerns with the headteacher or DSL.

6. Cyber-Bullying

Cyber-bullying is defined as online bullying through social media, messaging apps or gaming platforms ().

We ensure pupils:

- Understand what cyber-bullying is.
- Know how to report concerns.
- Know how to support peers.

Staff receive training on:

- Online harassment
- Image-based abuse
- AI-generated bullying content
- Anonymous messaging risks

Incidents follow the behaviour policy and may involve police if illegal content is present ().

7. Searching, Screening and Confiscation

Staff may search or delete data on pupil devices where there is a *good reason*, in line with:

- DfE Searching, Screening & Confiscation
- UKCIS Sharing Nudes & Semi-Nudes
- Education Act 2011 powers ()

Complaints follow the school complaints procedure.

8. Acceptable Use of ICT

All pupils, staff, volunteers, governors and visitors must follow the school's acceptable use agreements (Appendices 1–3) ().

9. Mobile Devices

Year 6 pupils may bring mobile devices but cannot use them during lessons, breaks or clubs (). Breaches may result in confiscation.

10. Staff Use of Work Devices

Staff must ():

- Use strong passwords.
- Keep devices encrypted.
- Install updates and security software.
- Use devices only for work.
- Report security concerns immediately.

11. Training

All staff receive:

- Online safety induction training ()
- Annual safeguarding refresher training
- Regular updates via email, bulletins and staff meetings

Training covers:

- Online abuse
- Cyber-bullying
- Radicalisation risks
- Image-based abuse
- AI-generated content risks
- Filtering & monitoring responsibilities

DSLs receive enhanced training at least every two years ().

Governors receive online safety training annually.

12. Monitoring and Review

- The DSL logs all online safety incidents (Appendix 5) ().
- Governors receive termly updates.
- Policy reviewed annually by the Headteacher.
- Annual online safety risk assessment informs updates.

APPENDIX 1: EYFS AND KS1 ACCEPTABLE USE AGREEMENT (PUPILS AND PARENTS/CARERS)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
When I use the school's ICT systems (like computers) and get onto the internet in school I will: ● Ask a teacher or adult if I can do so before using them ● Only use websites that a teacher or adult has told me or allowed me to use ● Tell my teacher immediately if: o I click on a website by mistake o I receive messages from people I don't know o I find anything that may upset or harm me or my friends ● Use school computers for school work only ● Be kind to others and not upset or be rude to them ● Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly ● Only use the username and password I have been given ● Try my hardest to remember my username and password ● Never share my password with anyone, including my friends. ● Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer ● Save my work on the school network ● Check with my teacher before I print anything ● Log off or shut down a computer when I have finished using it **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

APPENDIX 2: KS2, (PUPILS AND PARENTS/CARERS)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** ● Always use the school's ICT systems and the internet responsibly and for educational purposes only ● Only use them when a teacher is present, or with a teacher's permission ● Keep my username and passwords safe and not share these with others ● Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer ● Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others ● Always log off or shut down a computer when I'm finished working on it **I will not:** ● Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity ● Open any attachments in emails, or follow any links in emails, without first checking with a teacher ● Use any inappropriate language when communicating online, including in emails ● Log in to the school's network using someone else's details ● Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** ● I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission ● I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

APPENDIX 3: ACCEPTABLE USE AGREEMENT (STAFF, GOVERNORS, VOLUNTEERS AND VISITORS)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
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 checking with teachers first ● 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 ICT manager 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:**

APPENDIX 4: ONLINE SAFETY TRAINING SELF-AUDIT FOR STAFF (2026)

St John's Angell Town Primary School

This self-audit supports staff in identifying their confidence levels and training needs relating to online safety. It should be completed **annually** and reviewed by the DSL.

Staff Details

Field	Information
Name	_____
Role	_____
Date Completed	_____

Section 1: Understanding Online Risks

Area of Knowledge	Confident	Partly Confident	Not Confident
Understanding the four categories of online risk (Content, Contact, Conduct, Commerce)	☐	☐	☐
Recognising signs of online harm (bullying, grooming, radicalisation, exploitation)	☐	☐	☐
Understanding risks linked to AI-generated content (deepfakes, synthetic media)	☐	☐	☐
Understanding risks linked to anonymous messaging apps	☐	☐	☐
Understanding risks linked to gaming platforms and chat functions	☐	☐	☐
Understanding risks linked to social media use	☐	☐	☐

Section 2: Responding to Online Safety Concerns

Area of Practice	Confident	Partly Confident	Not Confident
Knowing how to report online safety concerns to the DSL	☐	☐	☐
Responding to disclosures involving online harm	☐	☐	☐
Following UKCIS guidance for incidents involving nudes/semi-nudes	☐	☐	☐
Managing cyber-bullying incidents	☐	☐	☐
Knowing when to involve external agencies (police, social care, Prevent)	☐	☐	☐
Understanding the school's filtering and monitoring expectations	☐	☐	☐

Section 3: Safe Professional Practice

Area of Practice	Confident	Partly Confident	Not Confident
Following the staff Acceptable Use Agreement	☐	☐	☐
Using school devices safely (passwords, encryption, updates)	☐	☐	☐
Understanding expectations around communication with pupils online	☐	☐	☐
Understanding data protection responsibilities when using digital tools	☐	☐	☐
Responding appropriately if harmful content is found on a pupil's device	☐	☐	☐

Section 4: Curriculum & Teaching

Area of Teaching	Confident	Partly Confident	Not Confident
Teaching online safety within Computing	☐	☐	☐
Teaching online safety within RSE/Health Education	☐	☐	☐
Embedding online safety across other subjects	☐	☐	☐
Adapting online safety teaching for SEND pupils	☐	☐	☐

Section 5: Training Needs

Tick any areas where further training would be helpful:

- ☐ Cyber-bullying
- ☐ AI-generated content and deepfake risks
- ☐ Filtering and monitoring systems
- ☐ Responding to nudes/semi-nudes incidents
- ☐ Online radicalisation and extremism
- ☐ Social media risks
- ☐ Gaming and online chat risks
- ☐ Data protection and digital security
- ☐ Supporting vulnerable pupils online
- ☐ Other (please specify): _____

Section 6: Additional Comments

Use this space to outline any concerns, questions or suggestions relating to online safety:

_____
_____
_____
_____
_____

1. APPENDIX 5: ONLINE SAFETY INCIDENT REPORT LOG

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**