

**ST JOHN THE BAPTIST C OF E
PRIMARY SCHOOL**

Online Safety Policy



Reviewed: February 2023

Next Review: February 2024

Person Responsible: Corrine Wellby

Agreed by: Standards and Curriculum



St John the Baptist C of E Primary School

Online Safety Policy

February 2023

Contents

| | |
|---|----|
| 1. Aims..... | 3 |
| 2. Legislation and guidance..... | 3 |
| 3. Roles and responsibilities..... | 3 |
| 4. Educating pupils about online safety..... | 5 |
| 5. Educating parents about online safety..... | 6 |
| 6. Cyber-bullying..... | 6 |
| 7. Acceptable use of the internet in school..... | 7 |
| 8. Pupils using mobile devices in school..... | 7 |
| 9. Staff using work devices outside school..... | 7 |
| 10. How the school will respond to issues of misuse..... | 8 |
| 11. Training..... | 8 |
| 12. Monitoring arrangements..... | 9 |
| 13. Links with other policies..... | 9 |
| Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)..... | 10 |
| Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)..... | 11 |
| Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)..... | 12 |
| Appendix 4: online safety training needs – self-audit for staff..... | 13 |
| Online Safety Contacts and References..... | 14 |

1. Aims.....

St John the Baptist Primary 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, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) 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 DfE'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.

3. Roles and responsibilities

3.1 The Governing Body

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

The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Adam Rockliffe

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 (appendix 3)

- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

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

3.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputy DSLs are set out in our child protection and safeguarding policy as well as 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, JSPC Computer Services and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged by the headteacher and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on CPOMS 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

This list is not intended to be exhaustive.

3.4 Computer Services (JSPC)

JSPC is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept 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 security check and monitoring the school's ICT systems on a fortnightly 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 by the headteacher 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

This list is not intended to be exhaustive.

3.5 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 (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure 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 dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)
- 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 resource sheet – [Childnet International](#)

3.7 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 (appendix 3).

4. Educating pupils about online safety

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

All schools have to teach:

- [Relationships education and health education](#) in primary schools

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

In **Key Stage 2**, pupils 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
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)?
- 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.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Parents will be invited to an annual Online Safety workshop in line with the E-Safety Day in February.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (E4S) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). 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.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Pupils using mobile devices in school

Pupils are allowed to bring personal mobile devices/phones to school but they must be handed to the school office for secure keeping until the end of the school day. At all times the device must be switched off or on silent. Parents must sign a permission slip before they can do this.

- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Headteacher.

10. 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 disciplinary procedures/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.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, harassing, and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputy/deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety via CPOMS.

This policy will be reviewed every year by the SLT. At every review, the policy will be shared with the Governing Board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

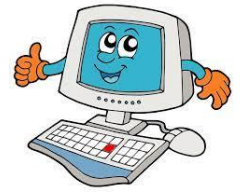
This online safety policy is linked to our:







- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy



KS1 Acceptance User Policy

To help me stay safe on the computer



| | | |
|---|---|--|
|  | <p>I will only use a computer if an adult tells me to.</p> | |
|  | <p>I will make sure that I only use my login details when working on a computer.</p> | |
|  | <p>I will keep my password safe and not share it with anyone.</p> | |
|  | <p>I will always send polite and kind messages.</p> | |
|  | <p>I will always tell an adult if I see something on the computer that makes me or my friends unhappy</p> | |
|  | <p>I will always log off or shut down the computer when I am finished working on it.</p> | |

Signed:

Dated:













Appendix 2: KS2 acceptable use agreement



KS2 Acceptance User Policy

To help me stay safe on the computer



| | | |
|---|---|--|
|  | I will ask permission before using the Internet and use it for a specific purpose. | |
|  | I will make sure that I only use my login details when working on a computer. | |
|  | I will never share my password with anyone. | |
|  | I will never share my personal details, such as my full name or address, with people I don't know. | |
|  | I will never meet up with someone I have met on the Internet. | |
|  | I will always check my messages are polite before I send them. | |
|  | I will not reply to a message that isn't kind, but I will save it and show it to an adult. | |
|  | I will not open or download a file unless I am sure it is safe. | |
|  | I know I should not believe everything I read on the Internet. | |
|  | I will always tell an adult if something on the Internet makes me or my friends unhappy | |
|  | I will not open any attachments in emails, or follow any links in emails, without first checking with a teacher | |
|  | I will always log off or shut down the computer when I am finished working on it. | |

Signed:

Dated:

Appendix 3: Acceptable Use Agreement (staff, governors, volunteers and visitors)



Staff Acceptance User Policy

To help me stay safe on the computer



| | |
|---|--|
| <ul style="list-style-type: none"> • I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body. • I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities. | |
| <p>Accessing computer systems</p> <ul style="list-style-type: none"> • I will not reveal my password(s) to anyone and will not record it in place where it could be easily discovered (such as the back page of a diary). • If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it. • I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems. | |
| <p>Data Protection</p> <ul style="list-style-type: none"> • I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and will do everything I can to protect the data from being accessed by unauthorised people. • I understand that the Data Protection Policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority. | |
| <p>Keeping children safe</p> <ul style="list-style-type: none"> • I will embed the school's e-safety curriculum into my teaching and teach children in my care about the e-safety and anti-cyberbullying rules. • I will be vigilant about e-safety risks and incidents (including cyber-bullying) that children in my charge might experience and respond promptly by following the agreed procedures and communicating concerns to the Computing Lead nominated child protection officer as appropriate. | |
| <p>Digital Images</p> <ul style="list-style-type: none"> • If I use personal digital cameras or camera phones for taking and transferring images of pupils or staff for professional purposes, I will save the photos on the school network and delete them from my equipment at the first available opportunity. • I will not store images or photos of children or staff at home without permission. • I will ensure that I do not photograph or video children for which release permission has not been granted. I will follow the school's guidance document on publication of photographs and videos. | |
| <p>Communications</p> <ul style="list-style-type: none"> • I will only use the approved, secure e-mail system(s) for any school business. • I will only use the approved school e-mail, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business. • I will use the school's Microsoft 365 account and any other school account in accordance with school. | |
| <p>Inappropriate Material</p> <ul style="list-style-type: none"> • I will not browse, download or send material that could be considered offensive. This could include (but does not exclusively include) materials that are pornographic, hateful, racist, sexist, abusive, obscene or discriminatory. • I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Computer Lead. • I understand that all Internet and network usage can be logged and this information could be made available to my manager on request. | |
| <p>Copyright</p> <ul style="list-style-type: none"> • I will not publish or distribute work that is protected by copyright. | |
| <p>Protecting the network & antivirus</p> <ul style="list-style-type: none"> • I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet if it does not have up-to-date anti-virus software (or been scanned first for USB flash drives), and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems. • I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed. | |
| <p>Personal use of online publishing systems</p> <ul style="list-style-type: none"> • I will not engage in any online activity that may compromise my professional responsibilities. • I will not make contact with children known to me through school on any social networking site. • I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role. | |

Signed:

Dated:

Appendix 4: Online safety training needs – self-audit for staff

| ONLINE SAFETY TRAINING NEEDS AUDIT | |
|--|------------------------------------|
| Name of staff member/volunteer: | Date: |
| Question | Yes/No (add comments if necessary) |
| Do you know the name of the person who has lead responsibility for online safety in school? | |
| Are you aware of the ways pupils can abuse their peers online? | |
| Do you know what you must do if a pupil approaches you with a concern or issue? | |
| Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors? | |
| Are you familiar with the school's acceptable use agreement for pupils and parents? | |
| Do you regularly change your password for accessing the school's ICT systems? | |
| Are you familiar with the school's approach to tackling cyber-bullying? | |
| Are there any areas of online safety in which you would like training/further training? | |

The Designated Safeguarding Lead (DSL) is Jane Sharrock (Headteacher), and the Deputy Safeguarding Lead is Tanya Stoner (SENDSCO).

The Online Safety Lead for the Governing Body is Adam Rockliffe.

Online Safety (e-Safety) Contacts and References

West Sussex Support and Guidance:

West Sussex County Council (Schools): www.schools.westsussex.gov.uk/

West Sussex Safeguarding Children Board (WSSCB): www.westsussexscb.org.uk/

E-Safety in West Sussex Schools:

www.westsussex.gov.uk/learning/west_sussex_grid_for_learning/management_info__services/it_support_for_schools/e-safety_in_west_sussex_school.aspx

Pan Sussex E-Safety Strategy:

<http://www.westsussexscb.org.uk/wp-content/uploads/Pan-Sussex-E-safety-strategy.pdf>

A Guide to Keeping Your Child Safe Online:

<https://www.westsussex.gov.uk/media/8523/online-safety-completed.pdf> 23

Sussex Police:

www.sussex.police.uk/

In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Sussex Police via 101

National Links and Resources:

- **Action Fraud:** www.actionfraud.police.uk
- **BBC WebWise:** www.bbc.co.uk/webwise
- **CEOP (Child Exploitation and Online Protection Centre):** www.ceop.police.uk
- **ChildLine:** www.childline.org.uk
- **Childnet:** www.childnet.com
- **Get Safe Online:** www.getsafeonline.org
- **Internet Matters:** www.internetmatters.org
- **Internet Watch Foundation (IWF):** www.iwf.org.uk
- **Lucy Faithfull Foundation:** www.lucyfaithfull.org
- **Know the Net:** www.knowthenet.org.uk
- **National Online Safety:** www.nationalonlinesafety.com/
- **Net Aware:** www.net-aware.org.uk
- **NSPCC:** www.nspcc.org.uk/onlinesafety
- **Parent Port:** www.parentport.org.uk
- **Professional Online Safety Helpline:** www.saferinternet.org.uk/about/helpline
- **The Marie Collins Foundation:** www.mariecollinsfoundation.org.uk/
- **Think U Know:** www.thinkuknow.co.uk
- **Virtual Global Taskforce:** www.virtualglobaltaskforce.com
- **UK Safer Internet Centre:** www.saferinternet.org.uk
- **360 Safe Self-Review Tool for Schools:** www.360safe.org.uk/
- **Online Compass (Self review tool for other settings):** www.onlinecompass.org.uk/