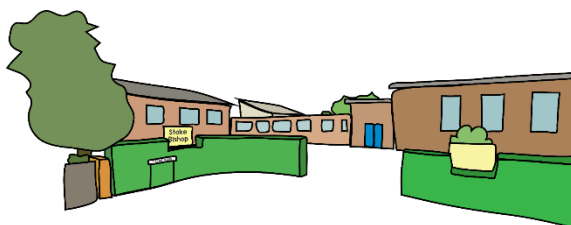


# Stoke Bishop CofE Primary School



## Online Safety Policy



### 'Believing it's Possible'

*Our community sits between two rivers that have historically supported growth and success. Working together with trust and passion, we learn, grow and thrive as we embrace the possibilities of life's journey:*

*Understanding that,*

*"Wherever the river flows, life will flourish" – Ezekiel 47:9*

**Approved by:**

Headteacher

**Date:** January 2024

**Last reviewed on:**

January 2024

**By:** Brinley Attewell (Computing Lead)

**Next review due by:**

January 2025

## 1. 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](#)
- [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.

This policy complies with our funding agreement and articles of association.

## 3. Roles and responsibilities

### 3.1 The governing board

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

The governing board 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 Sophie Summers, the Safeguarding Governor

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 approach to safeguarding and related policies and/or procedures

### 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 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 on CPOMS 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

This list is not intended to be exhaustive.

### 3.4 The ICT manager

The ICT manager 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 weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- 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

All staff, including contractors, students and agency staff, 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 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 and logged on CPOMS using the four C categories outlined in [KCSIE \(Keeping Children Safe in Education\) - P33, Para 124](#)

This list is not intended to be exhaustive.

### 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 factsheet - [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, ensuring coverage in line with the recommended framework '[Education for a Connected World](#)'.

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.

## 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 via the school website.

Online safety may also be covered during learning meetings and other information sharing events.

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 one 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

Within the whole school approach to online safety everyone will be aware of the breadth of issues to be addressed using the four C categories outlined in KCSIE (see appendix 4) including that of peer on peer abuse.

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 pupils as part of their learning around online safety.

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 (PSHE) education, and other subjects where appropriate.

As part of safeguarding training, all staff and governors 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 website also provides links to information on cyber-bullying for 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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

### 6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

## 7. Acceptable use of the internet in school

All staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendix 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Pupils' teacher will share with them, each year, the acceptable use agreement for their age group and agree as a class that these rules must be followed in school (appendices 1 and 2).

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, 2 and 3.

## 8. Pupils using mobile devices in school

Pupils in Year 6 may bring mobile devices into school on the condition that they are:

- Switched off at all times whilst on the school grounds
- Handed in to the class teacher at the beginning of the day and only collected at the end of the school day

Any breach of these conditions 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

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, as set out in appendix 3.

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.

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

Work devices must be used solely for work activities.

Any hard copy data (e.g. pupil records, planners, diaries etc) taken offsite must be suitably secured in both transit and at rest. For example, ensuring it is not on display when left in a vehicle - leaving documents in a vehicle overnight is not acceptable, and ensuring it is either locked away or out of sight when working from home.

## 10. Staff using personal/non-school devices (Bring Your Own Device)

Bring Your Own Device (BYOD) is the practice of allowing staff to utilise personally owned devices (such as smartphones, tablets or laptops) to securely access some or all of the school's systems, applications and services.

The following conditions apply to the use of this facility.

- Staff may only connect to the school's systems for the purpose of authorised work or their studies.
- Ideally use of a device that has access to the school's systems, applications and services via the BYOD facility should be limited to its owner and should not be shared. If it is necessary to share a device, the first user must ensure that they are logged out of their school account before handing over the device to a colleague/friend.
- Account logon, passwords and pin numbers for gaining access to the school's systems, applications and services that have been issued to individuals must remain confidential and never shared with others.
- No data from the school system may be downloaded and saved to a device. Similarly, data and information may not be downloaded to any storage device, such as a USB memory stick, that is

attached to the BYOD device that has been granted access. Staff should be conscious of where they are using their device. They should ensure data and systems displayed on the screen of the device are not visible to others. Screenshots of systems must not be taken.

- Staff must inform the School Business Manager if they leave employment with the organisation.
- Personal devices are brought into the school entirely at the risk of the owner. The school does not accept any liability for loss or damage of personal devices and data that are using the BYOD system. It is recommended that the owner (at their own expense) purchases an insurance policy to cover loss / theft / damage etc.
- The school accepts no responsibility for the day-to-day maintenance or upkeep of a user's personal device, nor for any malfunction of a device due to changes made to the device while on the school's network or whilst resolving any connectivity issues.
- The school recommends that all devices are made easily identifiable and have a protective case as the devices are moved around the school.
- Staff are solely responsible for all costs associated with purchasing, running, repairing and replacing their personal devices used with BYOD.
- Any charges relating to connecting a BYOD device to the school's systems, applications and services, such as using the data element of a mobile phone contract, are the responsibility of the device owner. It is recommended that Staff using mobile data or Wi-Fi hotspots should periodically monitor the flow of data to ensure that they have sufficient allowance. The school accepts no responsibility for the data required to provide those applications and services.
- While the school will take every precaution to prevent an employee's own data from being lost when the school needs to 'remote wipe' a device, it is the employee's responsibility to take precautions to protect their data and information, such as backing up emails, contacts, etc
- Confidential data should only be accessed for a specific work-related requirement.
- Printing hard copies of material containing personal data is strongly discouraged as it will create security and destruction issues.
- Hard copies may only be disposed of via the confidential waste bags in the school office.
- Images of pupils should be taken using school devices where possible. Where necessary, staff may use their own devices to take images or footage of students, but images must be deleted as soon as they are no longer required, saved securely on the school system and deleted in accordance with the retention policy.
- Staff should not save the personal numbers of students or parents to their devices and should contact parents/carers via the school office phones.
- Passwords must not be saved, either in a web browser on the device or written down and left in accessible places.
- Users must log out of programmes when they are no longer using them.
- The device may be remotely wiped if:
  - The device is lost
  - When a member of staff leaves the school
  - IT detects an incident, such as a data breach or a cyber incident, that presents a threat to the school's systems, applications and services.

In the case of data loss staff / students must immediately inform the School Business Manager if:

- Their password has been breached
- Their device is lost or stolen
- Organisational systems are not working normally - in those cases Bristol ICT support may choose to wipe data from the device in order to minimise risk of an impact on either the school's systems, applications and services.

## 11. 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 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.

## 12. 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).

The DSL 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.

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

## 13. Monitoring arrangements

The school logs behaviour and safeguarding issues related to online safety on CPOMs.

This policy will be reviewed annually as part of the review of Safeguarding procedures and the KCSIE document, in collaboration with the Computing Leader. At every review, the policy will be shared with the governing board.

## 14. Links with other policies

This online safety policy is linked to our:

- Safeguarding and Child protection Policy
- Behaviour policy
- Adult Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy



## Appendix 1: EYFS and KS1 acceptable use agreement for pupils

The following points must be shared with and understood by pupils in EYFS and KS1 at school.

### ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS

#### **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:
  - I click on a website by mistake
  - I receive messages from people I don't know
  - I find anything that may upset or harm me or my friends
  - I receive an email which doesn't look or feel right
- Use school computers for school work only
- I will 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

**Pupils should understand that the school will monitor the websites they visit and that there will be consequences if they do not follow the rules.**

## Appendix 2: KS2 acceptable use agreement for pupils

### ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS

#### **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 hand it into the school office at the beginning of the day
- I will ensure it is switched off whilst I am on the school grounds and will not switch it on until I have left

**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**

## 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, and note that recorded information is subject to the Data Protection Act and Freedom of Information Act and may be within scope of a request under both sets of legislation.
- 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, and checking the necessary consents each time a photo of a pupil(s) is to be used.
- 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
- Leave the device unlocked when left unattended
- Respond, click link(s) or open any attachments from emails which I was not expecting or do not look and feel right

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 needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
<b>Name of staff member/volunteer:</b>	<b>Date:</b>
<b>Question</b>	<b>Yes/No (add comments if necessary)</b>
Do you know the name of the person who has lead responsibility for online safety in school?	
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?	

## Appendix 5: Four 'areas of risk' outlined in Keeping Children Safe in Education 2021 published by Department for Education

**content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

**contact:** being subjected to harmful online interaction with other users; for example: 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; for example, 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; and •

**commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.