St Paul's Church of England Primary School

Internet Safety Policy

Date adopted:	March 2022		Last reviewed:	March 2024
Review cycle:	Every 1 year		Is this policy statutory?	No
Approval:	SLT		Author:	Eleanor Reid
Local approval*:			Local author*:	
Next review Date	March 2025			

* only for policy/procedures that are templates and require local adaptation.

Revision record

Minor revisions should be recorded here when the policy is amended in light of changes to legislation or to correct errors. Significant changes or at the point of review should be recorded below and approved at the level indicated above.

Revision No.	Date	Revised by	Approved date	Comments
1				

Contents

1. Aims 2
2. Legislation and guidance 2
3. Roles and responsibilities 3
4. Educating pupils about online safety 4
5. Educating parents/carers about online safety 5
6. Cyber-bullying 5
7. Acceptable use of the internet in school 6
8. Mobile devices in school 6
9. Social media usage 6
10. Managing emerging technology 7
11. Managing video conferencing 7
12. Email 7
13. Publishing pupil's images and work 7
14. Staff using work devices outside school 7
15. How the school will respond to issues of misuse 8
16. Training 8
17. Monitoring arrangements 8
18. Links with other policies 8
Appendix 1: Acceptable use agreement (pupils and parents/carers) 9
Appendix 2: Acceptable use agreement (staff, local governing committee members, volunteers and visitors) 11
Appendix 3: Online safety incident report log 14

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and local governing committee members
- 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 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 Local Governing Committee

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

The local governing committee 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).

All local governing committee members 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 2)

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

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 3) 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
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or local governing committee

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 half-termly basis

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

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 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 3) 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.

3.6 Parents/carers

Parents/carers 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/carers 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 2).

4. Educating pupils about online safety

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

The new relationships and sex education (RSE) curriculum became statutory as of the summer term 2021.

Under the new requirement, **all** primary schools will have to teach Relationships education and health education. (See the school's RSE policy.)

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

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

5. Educating parents/carers about online safety

The school will raise parents'/carers' awareness of internet safety in monthly newsletters, and in information via our website. This policy will also be shared with parents/carers.

If parents/carers 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

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. This will primarily be included through our Wellbeing curriculum.

All staff, local governing committee members and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 16 for more detail).

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 and the school's COVID-19 risk assessment.

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 pupils, parents/carers, staff, volunteers and local governing committee members are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-2). 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, local governing committee members and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Mobile devices in school

For the purposes of this policy, a mobile device is a portable computing device such as a smartphone, smart watch or a tablet computer (including iPads etc.). Mobile devices brought in to school are the responsibility of the device owner.

Pupils in year 5 and 6 (who are walking home alone) may bring mobile devices into school, but must hand them in when they arrive. These will be kept in a safe place and returned to them at the end of the school day.

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.

No images, videos or voice recordings of pupils should be taken on personally-owned mobile devices.

Staff will be advised to:

- Limit mobile phone usage to during break, lunch and PPA time.
- Ensure that Bluetooth or other forms of communication are hidden or disabled during lesson times.
- Keep mobile devices switched off or on silent mode during lesson times.
- Not use personal mobile devices during teaching periods. (See mobile device policy.)

9. Social media usage

Social media, which includes all apps and websites that allow sharing and communication between users, can be a valuable part of modern life. We acknowledge that many staff, parents/ carers and pupils will access social media. As such, we expect that everybody will behave in a positive manner, engaging respectfully with the school and each other. (See acceptable usage policy.) This includes not making any posts (either public or within private groups) that are or could be viewed as bullying, rude, insulting, illegal or otherwise inappropriate or which could bring the school into disrepute.

Many social media platforms have an age restriction of 13 years old. We ask that parents/ carers respect these age restrictions and do not encourage or condone social media usage. As a school, we acknowledge that some children may have access to these sites. Therefore, within online safety learning, the children will be taught about the risks of social media and how to behave appropriately online.

10. Managing emerging technology

Emerging technologies, such as smart watches with internet accessibility or camera functions are not to be used by pupils at school. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

11. Managing video conferencing

Videoconferencing will be carried out via school accounts. Children will be supervised when taking part in video calls. As a result of COVID-19 lockdowns, children may be accessing zoom sessions from home. Where this takes place, two members of staff will always be on the call. (See Remote Learning Code of Conduct.)

12. Email

All communication with parents/carers will be made through school email addresses. The following guidelines set out acceptable email usage:

- The forwarding of chain emails is not permitted.
- Email attachments should only be opened if the sender is known.
- All communication between staff and parents/carers should be professional in tone and content.
- Users should immediately report any communication that makes them feel uncomfortable or is offensive, discriminatory or threatening in tone.

13. Publishing pupil's images and work

Written permission will be obtained from the global permission forms when the pupil joins the school for pupil's images and work to be displayed on social media (e.g. Twitter), the school website and on our learning platforms (e.g. Seesaw). Where possible, group photos or photos where a pupil cannot be clearly identified will be used. Pupil's work can be only be published on the website or social media with the permission of the parents/carers.

Pupil's full names will not be used on the website and children will be encouraged to avoid using their full name or including personal details on the school learning platform. When using the school learning platform, each child has an individual login which can only be accessed by school staff and the individual child and their parents/carers.

14. 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
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install 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 2.

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 ICT Manager.

15. 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 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.

16. 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 and 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.

Local governing committee members 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 safeguarding and child protection policy.

17. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 3.

This policy will be reviewed every year by the Computing Leads. At every review, the policy will be shared with the local governing committee.

18. Links with other policies

This online safety policy is linked to our:

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

Appendix 1: Acceptable use agreement (pupils and parents/carers)

Internet and Computing Code of Conduct

At St Paul's we expect all pupils to be responsible for their own behaviour on the internet, just as they are anywhere else in school. This includes materials they choose to access and language they use.

These rules will keep everyone safe and help us to be fair to others.

- I will only use the school's computers for schoolwork and homework, unless the teacher tells me otherwise.
- I will only delete my own files.
- I will not look at other people's files without their permission.
- I will keep my logins and passwords secret and only use my own logins.
- I will always log out and close my browser when I leave the computer.
- I will not bring files into school without permission and if I bring my homework into school on a USB memory stick, it will have to be virus scanned by the teacher.
- I will not send, access, store or display offensive messages or pictures.
- I will ask permission from a member of staff before using the Internet and will not visit Internet sites that are not for my work. I will only access sites which are appropriate for use in school.
- I will not deliberately seek out offensive materials and should I encounter any such materials accidentally, I will report it to a teacher immediately.
- If I see, hear or read anything that I do not like or I receive a message that I am unhappy with or which makes me feel uncomfortable, I will not respond to it but I will tell a teacher / responsible adult.
- I will only e-mail people my teacher has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not use or send bad, threatening or annoying language nor any language which might incite hatred against any ethnic, religious or other minority.
- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
- I will not give my name, home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.

INTERNET AND COMPUTING CODE OF CONDUCT AGREEMENT

Pupil:

Name:_____ Date_____

Parent:

As parent or carer, I have read, discussed and explained the Internet and Computing Code of Conduct to my son/daughter. I understand that if he/she fails to follow this code I will be informed and internet access may be withdrawn,

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching e-safety skills to pupils.

Parent/Guardian Signature Date _____

Please Print Name _____

Appendix 2: Acceptable use agreement (staff, local governing committee members, volunteers and visitors)

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's Internet Policy and E-Learning Code of Conduct for further information and clarification.

1. The information systems are school property and I understand that they must be used appropriately in school. I agree to follow school guidelines as detailed in the Internet Policy and E-Learning Code of Conduct with regard to use of school information systems.
2. I will ensure that my information systems use will always be compatible with my professional role.
3. I understand that school information systems may not be used extensively for private purposes, without specific permission from the headteacher.
4. I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
5. I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager and I will follow the data protection regulations for staff.
6. I will only install new software or hardware with permission from the IT technician or IT leader.
7. I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely in accordance with the data protection regulation.
8. I will respect copyright and intellectual property rights.
9. I will report any incidents of concern regarding children's safety to the school IT leader or the headteacher as appropriate.
10. I will ensure that any electronic communications with pupils are compatible with my professional role.
11. I will promote E-safety with pupils in my care and will help them to develop a responsible attitude to system use regarding the content they access or create and to help them to stay safe in this environment.
12. I will not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with my professional role.
13. I will not accept current school pupils as friends on social networking spaces such as Facebook and I will not accept past pupils under 18 without the express permission of their parents.
14. Regarding social media, I will ensure that my privacy settings on all social networking sites are at an appropriate level and I understand that I must remain professional when accessing or interacting with social networking sites out of school hours. The use of social media will remain as part of my social life and I will not make any references to my place of work, any activities within the school or any work concerns that I may have.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Any reports of the inappropriate use of social media that are brought to the attention of school leaders will be investigated and may result in disciplinary action being taken.

Data Protections Regulations for Staff

The Data Protection Act says that: "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data." All staff must therefore ensure that they follow the data protection regulations below:

1. Password security

1.1. Passwords must contain a minimum of 8 characters; one of which must be a number, one must be a capital letter and one must be a lower-case letter.

1.2. Do not use obvious passwords e.g. Password1 – Arbor will reject obvious password automatically. Consider using a password with three random words combined e.g. Horsemanflower1

1.3. You will be forced to change your server password every 7 weeks. When the server password is changed you must change your email password and Arbor password at the same time. To change the Arbor password, click the options (small cog icon at the top right) and click reset password.

1.4. Do not allow your computer / electronic devices (either at home or in school) to save passwords – if this happens automatically this must be reported to the IT technician and rectified.

1.5. Passwords must not be shared, given to anyone other than the IT technician or given over the phone; Arbor's support team will never ask for a password. In exceptional circumstances a password may be shared by more than one member of staff but this must be approved by the IT technician and the password must remain only with those staff members authorised to have it. The only circumstances in which this will apply are sharing of a generic email address e.g. After school club@, parents@ etc. Arbor passwords must never be shared.

1.6. Passwords must not be written down, for example in your diary. Any document with a list of passwords must be stored safely e.g. in a locked filing cabinet or password protected if stored on the computer.

2. Data Security

2.1 When using any electronic device (either at home or at school), you must log off or Ctl Alt Del and lock the device when they leave it.

2.2 If you allow any other member of staff to use a PC logged on in your name, be aware that any confidential documents within your personal H drive will be available for them to open. Also be aware that if you allow a member of staff to use your Arbor account which you have logged on for them, you are ultimately responsible for any work carried out in your name.

2.3 The Arbor system contains all personal and sensitive data for all pupils in the school. You must therefore use it with the utmost care by ensuring that only authorised individuals are able to log on and view data.

3. Transfer of data

3.1 The transfer of any pupil or staff data must be done securely.

3.2 Any documents with any personal details of pupils or staff must be password protected.

3.3 Any documents with any personal details of pupils or staff that are emailed must be password protected and a separate email must be sent giving the password to open the document.

3.4 Memory sticks / external hard drives can be used however a list of any documents that contain personal data (and the nature of the personal data) of pupils or staff must be kept. Any documents with pupil or staff data must be password protected. An encrypted memory stick should be considered if the majority of the files on the memory stick contain personal data of pupils or staff.

3.5 Any hard files or electronic devices being taken home must not be left in a car.

4. Breaches of security

4.1. Any concerns regarding breaches of data security must be reported immediately to the IT technician and a member of SLT. If unsure, please report concerns. These may include: misuse of passwords, loss of data, loss or damage of any electronic device on which data is stored, loss of any hard files containing personal data etc

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

Appendix 3: 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**