



Ashton St. Peter's Church of England Voluntary Aided Primary School

E-Safety Policy

Ratified in September 2019

Update in September 2022

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

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

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

Roles and responsibilities

The governing board

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

The 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).

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 2)

The headteacher

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

The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy.

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 4) 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 3 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.

The Computing subject leader

The Computing subject leader is responsible for:

- Communicating with the school's Technical Support Assistant at Partnership Education to ensure that:
 - Appropriate filtering and monitoring systems are put in place, 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
 - The school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
 - Access to potentially dangerous sites are blocked and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

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 4) 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.

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 (appendix 1)

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

- What are the issues?, UK Safer Internet Centre: <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>
- Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>
- Parent factsheet, Childnet International: <http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf>

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).

Educating pupils about online safety

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

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

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

The school will dedicate half a term at the beginning of the academic year to the overt teaching of e-safety. These lessons aim to raise pupils' awareness of the dangers that can be encountered online and provide them with strategies for staying safe online. This information will be referred to throughout the year to ensure the children are using the internet safely and are confident about what they should do if they have concerns about online content.

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.

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.

Cyber-bullying

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.)

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 class, as part of their Computing lessons.

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.

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).

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.

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.

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 and 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.

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

Pupils using mobile devices in school

Pupils in Upper Key Stage 2 are permitted to bring mobile phones into school if they walk to or from school without an adult, in order to be contacted or make contact in an emergency. While they are in school, pupils must keep their mobile phones stored in their lockers and are not to use them during 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.

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 2.

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 school's Technical Support Assistant at Partnership Education.

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 the behaviour policy. 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. 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.

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.

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.

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

Review Procedures

The School's policy will be reviewed:

- Every three years – next date September 2022
- When the School wishes to review the policy.
- If amendments are required by the LA

Ratified by:

Date: September 2019

Chair of Governors

Appendix 1



Pupils' Internet Safety Rules

RULES FOR ONLINE SAFETY AT ASHTON ST. PETER'S CHURCH OF ENGLAND VA SCHOOL

I will always ask the teacher before I use the Internet and will be sensible whenever I use it.

I will only use the Internet for schoolwork and will only use the sites my teacher has asked me to access.

I will not give my name, address or telephone number to anyone on the Internet and I will tell the teacher if anyone asks me for my name, address or telephone number.

I will never agree to meet someone I have spoken to on the Internet.

I will not download programs or bring programs on disc or CD Rom from home into school.

I will only e-mail the people my teacher has approved and the messages I send will be polite and responsible.

I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself.

I realise that if I don't use the Internet sensibly I will not be allowed to use it.

Appendix 2



Ashton St. Peter's Church of England Voluntary Aided Primary School

Acceptable IT Use Statement for Staff Policy To be read with 'Staff Behaviour Policy' and 'E-Safety Policy'

Ratified in October 2017
Update in October 2020

Computer Systems

The computer system, including hardware is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's 'E-Safety Policy' has been drawn up to protect all parties – the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited or emails received or sent.

Staff should sign a copy of this 'Acceptable IT Use Statement' and return it to the school office for storage in Personnel Files.

The following applies whilst staff laptops are connected to either the school network or the internet via an out of school hub;

- **All Internet activity should be appropriate to staff professional activity**
- **Access should only be made via the authorised account and password, which should not be made available to any other person**
- **Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden**
- **Any activity that brings the school into disrepute, such as the inappropriate use of social networking sites is forbidden**
- **Accessing and using social network sites is forbidden**
- **Users are responsible for all email sent and for contacts made that may result in email being received**
- **Use for personal gain, gambling, political purposes or advertising is forbidden**
- **Copyright of materials must be respected**
- **Posting anonymous messages and forwarding chain letters is forbidden;**
- **As email can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media**
- **Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden**
- **Any email attachments (documents, programs, pictures etc) must be checked for virus content before being opened**
- **Random monitoring of equipment and hardware will take place**
- **Any breach of the above may lead to disciplinary action**

Mobile Telephones

All teaching, non-teaching, clerical and site staff must ensure:

- **Telephones are on silent or switched off and stored in bags**
- **Telephones are used before 8.45am, at break-times, lunchtimes or after school hours**
- **Cameras on telephones should not be used under any circumstances to photograph children in or outside of school**
- **Photographs of children can only be taken on cameras or video cameras provided by school**
- **Any breach of the above may lead to disciplinary action**

I agree to adhere to this policy

Name:

Signed:

Date:

Review Procedures

The School's policy will be reviewed when:

- **Every 3 years October 2020**
- **The School wishes to review the policy**
- **If amendments are required by the LA**

Ratified by:

Date: October 2019

Chair of Governors

Appendix 3

Computing questionnaire

Please answer really honestly. Your answers are only for me and I want to be able to help as much as I can!

How often do you manage to teach computing?

Do you teach computing or is it left as PPA cover?

Looking at the LTP, which units do you feel most confident teaching?

Which units do you feel you need more support with?

If you need support, what in particular would you like help with? (finding resources/using correct vocabulary/creating a sequence of lessons)

What could teachers in previous year groups do to ensure your class are where they need to be for your lessons?

What else could be done to improve your experience of teaching computing?

Appendix 4

Date of Incident	Description	Immediate corrective action	Further action	Legal Implications	