St Anne's C.E. (Aided) Primary School

Online Safety Policy

Updated September 2023

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 2022', 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.

Online Safety

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **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. If we feel your pupils, students or staff are at risk, we will report it to the Anti-Phishing Working Group (https://apwg.org/).

We aim to ensure online safety is a running and interrelated theme in our policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead and any parental engagement.

Roles and responsibilities

The governing body

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. They also have an understanding the expectations, applicable roles, and responsibilities in relation to filtering and monitoring.

The designated safeguarding lead

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

The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- Working with the Computing leader, technical support and other staff, as necessary, to address any online safety issues or incidents;
- Ensuring that any online safety incidents are logged using Smoothwall and/or CPOMs 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 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 governing body.

This list is not intended to be exhaustive.

The ICT Technical Support (Fingertips Solutions)

The ICT Technical Support 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, with unreasonably impacting on teaching and learning;
- Reviewing filtering and monitoring provision at least annually;
- 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.

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy;

- Implementing this policy consistently;
- Understand their own roles and responsibilities around filtering and monitoring;
- 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 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 ***Computing*** 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.

Through ***Relationships Education***:

Online relationships

Pupils should 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.

and Health Education:

Internet safety and harms

Pupils should know

- that for most people the internet is an integral part of life and has many benefits.
- about the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.
- how to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.
- why social media, some computer games and online gaming, for example, are age restricted.
- that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health.
- how to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted.
- where and how to report concerns and get support with issues online.

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.

Educating parents about online safety

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

Online safety may also be covered during parents' evenings.

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.

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.

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 receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. We also send 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 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

Online risks are posed more by behaviours and values than the technology itself . 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.

Adults must use only equipment and internet services provided by the school so they must:

▪ turn off 3G/4G data access on school premises;

▪ follow the school's Acceptable Use agreement (see Appendix 2)

▪ ensure that their use of technologies could not bring their employer into disrepute

▪ not discuss or share data relating to children/ parents / carers in staff social media groups

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 and 2.

Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Off site visits
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

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.

Remote Learning

Where children are expected to learn at home in line with our Remote Learning Policy, we will provide a device as part of a loan agreement for use at home. Access will be granted to school systems. Children and parents are expected to sign the Acceptable Use Policy before devices are provided

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. Any USB devices must not be used.

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

Work devices must be used solely for work activities.

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 every three years as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings).

The DSL and deputy 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.

Filtering and Monitoring arrangements

Whilst providing children with a safe environment in which to learn, we will be doing all that we reasonably can to limit children's exposure to risks from the school's IT system. As part of this process, we implement monitoring systems through a monitored Firewall and also the use of Smoothwall to detect any inappropriate use of the internet.

All staff have a responsibility to log behaviour and safeguarding issues related to online safety on CPOMs which will be monitored by the DSL.

Useful Resources

DfE advice for schools: teaching online safety in schools

UK Council for Internet Safety (UKCIS) guidance: Education for a connected world

UKCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people

The UKCIS external visitors guidance will help schools and colleges to ensure the maximum impact of any online safety sessions delivered by external visitors.

National Crime Agency's CEOP education programme: Thinkuknow

Public Health England[38]: Every Mind Matters

Harmful online challenges and online hoaxes - this includes advice on preparing for any online challenges and hoaxes, sharing information with parents and carers and where to get help and support.

Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Conduct Policy
- Staff Disciplinary Procedures
- Data Protection Policy and Privacy Notices
- Complaints Procedure

Acceptable Use Policy

Early Years and Key Stage 1

I understand that St Anne's Acceptable Use Policy will help keep me safe and happy online whether I am using school devices or my own personal devices.

- I only use the internet when an adult is with me.
- I only click on links and buttons online when I know what they do.
- I keep my personal information and passwords safe.
- I only send messages online which are polite and friendly.
- I know that St Anne's staff can see what I am doing online when I use computers and tablets and Tapestry, Google Classrooms, Purple Mash, Timetables Rock Stars, including when I am at home.
- I always tell an adult if something online makes me feel upset, unhappy, or worried.
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online.
- I know that if I do not follow the rules my teacher will:
    - restrict or remove access to the internet, my remote learning platform and devices,
    - inform my parents/carers,
    - only give me access to hard copies of my school work.
- I have read and talked about these rules with my parents/carers.

Key Stage 2

I understand that St Anne's Acceptable Use Policy will help keep me safe and happy online at

home and at school.

Safe

- I will behave online the same way as I behave in the classroom.
- I only send messages which are polite and friendly.
- I will only post pictures or videos on the internet if they are safe and appropriate, and if I have permission.
- I only talk with and open messages from people I know.
- I will only click on links if I know they are safe.
- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.
- I will always be myself and not pretend to be anyone or anything I am not.

Learning

- I will use tablets, laptops, chrome books to access online learning.
- I will not use a personal device to access the internet and only use school equipment.
- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen.
- I use school devices for school work.
- If I need to learn online at home, I will follow the school remote learning AUP.

Trust

- I know that not everything or everyone online is honest or truthful.
- I will check content on other sources like other websites, books or with a trusted adult.
- I always credit the person or source that created any work, images, or text I use.

Responsible

- I keep my personal information safe and private online.
- I will keep my passwords safe and will not share them.
- I will log off when I have finished using the computer or device.
- I will not access or change other people's files or information.
- I will only change the settings on a device if a member of staff has allowed me to.
- I will not look for bad language, inappropriate images or violent or unsuitable games and, if I accidently come across any of these, I will report it to a teacher or adult in school, or a parent or carer at home.
- If, for any reason, I need to bring my mobile phone into school, I know that it is to be handed in to the office and then collected at the end of the school day.

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that all school devices and systems are monitored to help keep me safe, including when I use them at home.
- I have read and talked about these rules with my parents/carers.
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online.
- I know that if I do not follow the school rules then:
    - restrict or remove access to the internet, my remote learning platform and devices,
    - inform my parents/carers,

- contact the police if a criminal offence has been committed.
- only give me access to hard copies of my school work.

Tell

- If I see anything online that I should not or that makes me feel worried or upset, I will minimise the page and tell an adult straight away.
- If I get unpleasant, rude, or bullying emails or messages, I will report them to a teacher or other adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.
- If I am aware of anyone being unsafe with technology, I will report it to a teacher.
- I know it is not my fault if I see or someone sends me something bad online. I always talk to an adult if I am not sure about something or if something happens online that makes me feel worried or frightened.

St Anne's Remote Learning AUP

I understand that:

- these expectations are in place to help keep me safe when I am learning at home using Google Classrooms, Zoom, Purple Mash, Timetables Rock Stars and Tapestry.
- I should read and talk about these rules with my parents/carers.
- remote learning will only take place using Google Classrooms, Zoom, Purple Mash, Timetables Rock Stars and during usual school times.
- My use of Google Classrooms, Zoom, Purple Mash, Timetables Rock Stars is monitored to help keep me safe.

2. Only members of St Anne's community can access Google Classrooms, Zoom, Purple Mash, Timetables Rock Stars.
    - I will only use my St Anne's provided login details to access remote learning.
    - I will use privacy settings as set up the school.
    - I will not share my login/password with others.
    - I will not share any access links to remote learning sessions with others.

3. When taking part in remote learning I will behave as I would in the classroom. This includes:
    - Using appropriate language.
    - Not taking or recording any images or content.
    - Not sharing images or other work as my own.
    - Having an appropriate avatar.

4. When taking part in Zoom sessions I will:
    - Mute my microphone when asked to.
    - Wear appropriate clothing and be in a suitable place.
    - Ensure backgrounds are neutral and personal information is not visible.
    - Use appropriate alternative backgrounds.
    - Attend the session in full. If for any reason I cannot attend a session in full, I will let my teacher know.

- Attend lessons in a shared/communal space or room with an open door and/or where possible when I can be supervised by a parent/carer or another appropriate adult.
- Have my own name as a screen name.

5. If I am concerned about anything that takes place during remote learning, I will:
    - Report my concerns to my teacher and tell a parent/carer.

6. I understand that inappropriate online behaviour or concerns about my safety during remote learning will be taken seriously. This could include:
    - Restricting or removing access to my remote learning platform and devices,
    - Informing my parents/carers,
    - My teacher contacting police if a criminal offence has been committed.
    - Only having access to hard copies of my school work.

St Anne's Acceptable Use of Technology Policy – Learner Agreement

I, with my parents/carers, have read and understood the *St Anne's* Acceptable Use of Technology Policy (AUP) and remote learning AUP.

I agree to follow the AUP when:

1. I use St Anne's devices and systems, both on site and at home.
2. I will not use my own devices in St Anne's, including mobile phones, gaming devices, and cameras.
3. I may use my own equipment outside of St Anne's, including communicating with other members of the school or when accessing school remote learning systems.

Name…… Signed…….

Class…… Date…….

Parent/Carers Name……..…….....

Parent/Carers Signature…….

Date……..…….

Appendix 2: Acceptable Use Agreement (staff, governors, volunteers and visitors)

Acceptable use of the St Anne's ICT systems and the internet

Agreement for Staff, Governors, Volunteers and Visitors

Name of staff member/governor/volunteer/visitor:

When using the St Anne's ICT systems and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to, material of a violent, criminal or pornographic nature
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the school's network using someone else's details

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 will connect to the school's WiFi and disconnect 3G/4G data access on my mobile phone or personal device.

I agree that the school will monitor the websites I visit.

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) 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 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
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? Please record them here.	