ST ANNE'S CE PRIMARY SCHOOL

E-Safety Policy

'…these three remain: faith, hope & love; and the greatest of these is love.' 1 Cor 13:13

Rooted in faith, family & friendship.
Growing in hope & aspiration.
Flourishing in love.

friendship ★ hope ★ compassion ★ forgiveness ★ trust ★ thankfulness

CONTENTS

Section 1: Aims

At St Anne's CE Primary School, we feel that engaging and supporting parents and children to improve their own understanding of e-safety issues is of great importance so that they can use and support each other when using the internet and all digital media, in a safe and secure way.

Our school aims to:

- have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- identify and support groups of pupils that are potentially at greater risk of harm online than others
- deliver an effective approach to online safety which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

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

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

We strongly believe that the use of the internet and email is hugely worthwhile and an essential learning tool for our pupils as they grow up in the modern world. However, because there are always concerns about children having access to undesirable materials, we have taken positive steps to deal with this risk in school. We aim to work in partnership with children, parents and carers to support them in their use of the internet, both at school and at home. Everyone working in or for our school shares an objective to help keep children and young people safe by following statutory outlines in:

- Keeping children Safe in Education
- DfE Teaching Online Safety in Schools
- Education for a Connected World framework.

Our school's internet access provider operates the ARK filtering system which restricts access to inappropriate materials. In addition to this, children are educated through the Computing curriculum on how to report any inappropriate material seen. All children in school are encouraged to follow the SMART rules to keep themselves safe online.

As part of promoting e-safety in school, we participate in Safer Internet Day every year in February. This program involves all children and aims to empower young people to take control of their digital lives. It also provides adults with up-to-date resources to keep pace with technological and online changes.

Section 2: Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships education
- Searching, screening and confiscation

It refers to the DfE's guidance on protecting children from radicalisation. It also 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.

Section 3: Roles and Responsibilities

At St Anne's CE Primary School all staff, governors and volunteers are responsible for e-safety. They should be proactive in addressing isues which arise and be confident in promoting the school's message of e-safety in the local and wider community.

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 body will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring. The governing body will also make sure that all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children. The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL). They will also monitor how children are taught to keep themselves and others safe, including keeping safe online.

The governing body must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. They will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- reviewing filtering and monitoring provisions at least annually
- blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- having effective monitoring strategies in place that meet their safeguarding needs

All governors will:

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

3.2 The headteacher

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

3.3 The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL) are set out in our Child Protection and Safeguarding Policy, as well as relevant job descriptions.

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

- supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- working with the headteacher and governing body to review this policy annually and ensure the procedures and implementations are updated and reviewed regularly
- taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- working with the ICT manager to make sure the appropriate systems and processes are in place
- working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- managing all online safety issues and incidents in line with the school's Safeguarding & Child Protection Policy
- 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 logged and dealt with appropriately in line with the school Behaviour Policy
- updating and delivering staff training
- 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
- undertaking annual risk assessments that consider and reflect the risks children face
- providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

3.4 The ICT Manager

The ICT manager is responsible for:

- putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- conducting full security checks 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 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.

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, and ensuring that pupils follow the school's terms on acceptable use
- knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by informing the DSL
- following the correct procedures by asking the DSL if they want to request bypassing the filtering and monitoring systems for educational purposes
- 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
- responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

3.6 Parents/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 the Parental Permissions & Information form

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
- Parent resource sheet – Childnet

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 and are expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Section 4: Educating Children about Online Safety

At St Anne's CE Primary School, the use of the internet is an integral part of both our Computing curriculum and the wider school curriculum. It serves as a powerful tool for research, exploration, and idea validation. However, we acknowledge that understanding and using the internet effectively is not something that can be easily grasped. It requires constant explanation and monitoring due to its ever-changing nature.

The use of the internet is not only a discretionary choice, but it is also a mandatory component of our curriculum. It is a vital tool that benefits our staff, students, and young people by providing access to an extensive range of educational resources worldwide. This includes art galleries and museums, as well as the opportunity to connect with specialists in various fields.

In Key Stage (KS) 1, pupils will be taught to:

- use technology safely and respectfully, keeping personal information private
- identify where to go for help and support when they have concerns about content or contact on the Internet or other online technologies.

In Key Stage (KS) 2, pupils will be taught to:

- use technology safely, respectfully and responsibly
- recognise acceptable and unacceptable behaviour
- identify a range of ways to report concerns about content and contact.

By the end of primary school, pupils will know:

- that people sometimes behave differently online, including by pretending to be someone they are not
- that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- how to critically consider their online friendships and sources of information, including awareness of the risks associated with people they have never met
- how information and data is shared and used online
- what sorts of boundaries are appropriate in friendships with peers and others, including in a digital context
- how to respond safely and appropriately to adults they may encounter, whom they do not know, in all contexts (including online).

Section 5: Educating Parents/Carers bout Online Safety

At St Anne's CE Primary School, we will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or Class Dojo. This policy will also be shared with parents/carers. Online safety will also be covered during Parents' Evenings where applicable.

The school will let parents/carers know:

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

If parents/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.

Section 6: Cyber-Bullying

Cyber-bullying occurs online, primarily through social networking sites, messaging apps, or gaming platforms. Similar to other types of bullying, it involves repetitive and intentional harm inflicted by one individual or group onto another individual or group.

6.1: Preventing and Addressing Cyber-Bullying

At St Anne's CE Primary School, 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 year goups. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes in Personal, Social, Health and Eduction (PSHE), 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.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school's 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 Designated Safeguarding Lead (DSL) will promptly report the incident to the police and provide them with the necessary evidence if there are reasonable grounds to believe that the possession of the material is illegal. Additionally, the DSL will collaborate with external services if it is determined to be necessary.

6.3 Examining Electronic Devices

The headteacher, along with any member of the Senior Leadership Team (SLT), has the authority to conduct a search and confiscate electronic devices if they have reasonable grounds to suspect that the device:

- poses a risk to staff or pupils
- is listed as a banned item in the school rules, thus allowing for a search
- contains evidence related to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or DSL
- explain to the child why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- seek the pupil's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated, where they believe there is a 'good reason' to do so. When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- engage in illegal activities
- violate school procedures or guidelines
- access inappropriate content
- pose a threat to the safety and well-being of induviduals within the school community.

If inappropriate material is found on the device, it is up to the headteacher or DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may prove as evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as practically possible. If the material is not believed to be evidence related to an offense, staff members may delete it under the following circumstances:

- reasonable suspicion that the material's continued exsistence may cause harm to any individual
- refusal by the pupil and/or their parent/carer to delete the material themselves.

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- not view the image
- confiscate the device and report the incident to the DSL immediately, who will decide what to do next.

The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- the DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- our Behaviour Policy

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

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. We recognise that AI has many uses to help pupils learn, but may also have the potential to be misuesd and used to bully others. For example, in the form of 'deepfakes', where AI is used to create and generate images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness. At St Anne's CE Primary School, we will treat any use of AI to bully pupils in line with our Anti-Bullying and Behaviour Policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Section 7: Acceptable Use of the Internet in School

At St Anne's CE Primary School, all pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read the school's terms on acceptable use if relevant.

The use of the school's internet must be for educational purposes and/or for the purpose of fulfilling the duties of an individual's role only.

We will monitor the websites visited by pupils, staff, volunteers, governors and (where relevant) visitors, makig sure they comply with the above and restricted access through filtering systems where appropriate.

Section 8: Pupils using Mobile Devices in School

Pupils in Year 5 and 6 may bring mobile devices into school, but are not permitted to use them during:

- lessons
- break/lunch times
- clubs before or after school, or any other activities organised by the school.

Pupils should only bring a mobile device into school if they need it to walk home independently. If a child is unsure about walking home, and there has been no prior indication from the parent/carer made to the office, the child's class teacher may permit the child to contact their parents using their mobile

device before leaving the school grounds (under supervision). If the school has not received permission from the pupil's parent/carer to allow the pupil to walk home independently, then the individual is not required to bring a mobile device into school.

Any breach of the Parental Permissions & Information Form (signed by the child and parent/carer) and the statements above by a pupil may result in disciplinary action in accordance with the school Behaviour Policy.

Section 9: Staff using Work Devices Outside School

At St Anne's CE Primary School, all staff members with access to a work device will take appropriate steps to ensure that their device remains secure. This includes:

- ensuring that the device has a password. Strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters
- not sharing the device among family or friends
- making sure the device automatically locks after being inactive for a period of time
- installing anti-virus and anti-spyware software
- keeping operating systems up to date, making sure that the latest update has been installed.

Staff members must not use their device in any way that would violate the school's terms of acceptable use, alongside our Staff Code of Conduct.

If staff have any security concerns about their device, they must seek advice form the ICT manager.

Section 10: How the School will Respond to Issues of Misuse

Where a pupil misuses the school's ICT systems or the internet, we will follow the procedures set out in our Behaviour Policy. The action will be dependent on the individual circumstances, nature and seriousness of the specific indicent.

Where a staff member misuses the school's ICT systems, the internet or a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct and staff disciplinary procedures in place. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will take into consideration whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Section 11: Training

At St Anne's CE Primary School, all new staff members will receive training, as a part of their introduction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisaton.

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

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

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

Training will also help staff to:

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

The DSL and Deputy 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.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

Section 12: Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety, using the school's safeguarding record system (CPOMS).

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

Section 13: Links with other Policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour olicy
- Staff Disciplinary Procedures
- Data Protection Policy
- Privacy Notice for Pupils, Parents & Carers
- Privacy Notice for Staff & Volunteers
- Complaints Procedures

Any questions or concerns regarding this policy should be made to
Name: **Mr Harry Larter**
Role: **Computing Subject Lead**
Date: **February 2024**