



# E-Safety Policy

January 2026

***WALKING IN LOVE,  
INSPIRING TRANSFORMATION***



## I: Vision and Aims

At St Anne's CE Primary School, we are committed to creating a safe, respectful and nurturing online environment for all members of our school community. Rooted in Christ, we walk in love (Ephesians 5:2), nurture a community of belonging, and encourage everyone to shine their light (Matthew 5:16).

As a Church of England school, our approach to online safety is firmly grounded in our Christian vision and values of **Compassion, Curiosity and Confidence**, which are embedded throughout this policy.

- **Compassion** underpins our expectation that all members of the school community behave with kindness, respect and responsibility online, showing care for themselves and others in all digital interactions.
- **Curiosity** supports children to explore, learn and create safely using technology, developing the knowledge and skills needed to navigate the digital world thoughtfully and responsibly.
- **Confidence** empowers pupils to make positive choices online, speak up when something does not feel right, and seek help when needed, enabling them to contribute to a safe and inclusive digital community.

We believe that the internet and digital technologies are essential tools for learning in the modern world. Alongside the benefits, we recognise the risks that children may face online. This policy sets out our commitment to safeguarding pupils by promoting safe practice, clear procedures and a shared responsibility between school, pupils, parents and carers.

By working in partnership with families and the wider community, we aim to educate, protect and empower all children to use technology safely, responsibly and confidently, both in school and beyond.

## 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 2026 guidance on [Mobile phones in schools](#) and DfE 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 considers 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 issues 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 IT 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) and Deputy Designated Safeguarding Leads (DDSL) are set out in our Child Protection and Safeguarding Policy, as well as relevant job descriptions.

The DSL & DDSLs take 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 IT manager to make sure the appropriate systems and processes are in place
- Working with the Headteacher, IT 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, to continue to provide them with relevant skills and knowledge to safeguard effectively.

### **3.4 The IT Manager (ARK)**

The IT 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 IT 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 IT 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 IT 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 IT 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**

### **4.1 Pupils will be taught about online safety as part of the curriculum**

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.
- Be discerning in evaluating digital content

By the end of primary school, pupils will know:

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this





- That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

#### **4.2 Pupils will be taught practical cyber security skills**

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

### **Section 5: Educating Parents/Carers about 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 any member of staff or the Headteacher.

### **Section 6: Cyber-Bullying**

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 1 person or group by



another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

### 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 groups. 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 Education (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, or staff authorised by the Headteacher (including members of the Senior Leadership Team), has the statutory authority to search for and confiscate electronic devices where they have **reasonable grounds** to suspect that the device:

- poses a risk to staff or pupils
- is a prohibited or banned item under the school's Behaviour Policy
- contains evidence relating to an offence
- has been, or could be, used to breach school rules or cause harm

These powers are exercised in accordance with the **Education Act 2011**, the **Education and Inspections Act 2006**, and the Department for Education's statutory guidance *Searching, Screening and Confiscation*.

#### Before a Search

Where a search is deemed necessary, authorised staff will, wherever possible and appropriate:

- assess the **urgency** of the situation and the potential risk to pupils and staff
- seek advice from the Headteacher or the Designated Safeguarding Lead (DSL) if the matter is not urgent
- explain to the pupil why the search is taking place, how it will be conducted, and allow them to ask questions
- seek the pupil's cooperation

All searches will be carried out in a manner that is **reasonable, proportionate, and respectful**, considering the age, needs and understanding of the pupil.

#### Examination of Data and Files





Authorised staff members may **examine data or files** on a confiscated electronic device where they have a **good reason** to do so. A good reason may include reasonable suspicion that the device has been, or could be, used to:

- engage in illegal activity
- access or share inappropriate or harmful content
- breach school policies or procedures
- pose a risk to the safety or wellbeing of any member of the school community
- disrupt teaching or undermine the safe environment of the school

When examining data or files, staff will:

- only access information **directly relevant** to the reason for the search
- act in accordance with **data protection principles**, including minimisation and confidentiality
- ensure decisions and actions are **recorded appropriately**

### **Deletion of Data and Files**

In **exceptional circumstances**, authorised staff may erase data or files from an electronic device. Before doing so, they will consider whether the material:

- may be required as **evidence** relating to a suspected offence
- raises a **safeguarding concern**

Where material is suspected to be evidence of an offence, it **must not be deleted**, and the device will be passed to the police as soon as reasonably practicable.

If the material is not believed to constitute evidence of an offence, staff may delete it where there is reasonable suspicion that:

- the continued existence of the material may cause harm to any individual
- the pupil and/or their parent/carer refuses to delete the material themselves
- the material undermines the safe environment of the school or disrupts teaching

Any deletion of data will be proportionate, justifiable, and recorded.

### **Indecent Images and Safeguarding**

If a staff member suspects that an electronic device contains an **indecent image of a child** (including nude or semi-nude images), they will:

- **not view** the image
- confiscate the device immediately
- report the matter to the **Designated Safeguarding Lead (DSL)** without delay

Staff must not copy, print, store, share or forward such images under any circumstances.

The DSL will act in line with:

- *DfE Searching, Screening and Confiscation guidance*
- *UK Council for Internet Safety (UKCIS) – Sharing nudes and semi-nudes: advice for education settings*
- *Keeping Children Safe in Education*

### **Record-Keeping and Parental Communication**

Appropriate records will be kept of:

- The reasons for the search
- Any examination or deletion of data
- Safeguarding actions taken

Parents/carers will be informed of incidents involving searches or confiscation where appropriate, unless doing so would place a child at risk.

### **Complaints**





Any complaints about searching, examining, or deleting data from electronic devices will be managed in accordance with the school's **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 misused 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 IT 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, making sure they comply with the above and restricted access through filtering systems where appropriate.

### **Section 8: Pupils using Mobile Devices in School**

St Anne's CE Primary School is a **mobile-free school**. Pupils are not permitted to use mobile phones or smart devices at any point during the school day. This approach supports safeguarding, wellbeing, learning, and positive behaviour.

In exceptional circumstances only, pupils in Year 5 and Year 6 may be permitted to bring a mobile device into school where this is necessary to support independent travel home.

Pupils are **not permitted to use mobile devices during the school day**. This includes:

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

Mobile devices must remain always switched off and out of use while pupils are on the school premises or taking part in school activities.

Pupils should only bring a mobile device into school if they **need it to walk home independently** and where **prior permission has been given by the parent/carer and recorded by the school**.





If a child is unsure about walking home independently and there has been no prior confirmation from the parent/carer, the child's class teacher may permit the pupil to contact their parent/carer using their mobile device **under staff supervision** before leaving the school premises.

If the school has **not** received permission from the pupil's parent/carer to allow the pupil to walk home independently, the pupil **should not bring a mobile device into school**.

If a pupil needs to bring a mobile device into school, they must follow these procedures:

- Pupils must switch their mobile device off before entering the school gate.
- Pupils must hand their device to a member of staff on arrival, who will check that it is switched off.
- Mobile devices will be stored securely and locked away by a member of staff throughout the school day.
- Devices will be returned to pupils at the end of the school day.
- All mobile devices must be clearly labelled with the pupil's name. Any unlabelled devices will be taken to the school office and must be collected by a parent/carer.

The school accepts **no responsibility for the loss, damage, or data held on personal mobile devices** brought into school.

Any breach of the Parental Permissions & Information Form, or of the expectations outlined above, may result in disciplinary action in line with the school's **Behaviour Policy** and may include the **confiscation of the mobile device**, in accordance with the Education Act 2011 and DfE guidance on searching, screening and confiscation.

Where the misuse of a mobile device raises a **safeguarding or online safety concern**, the matter will be dealt with in line with the school's **E-Safety Policy, Child Protection Policy**, and relevant safeguarding procedures.

Parents and carers should note that pupils will not use mobile phones to contact home during the school day. Messages to or from pupils must be communicated via the school office.

Reasonable adjustments will be made for pupils with medical needs, disabilities or safeguarding requirements, in line with the Equality Act 2010. Any such adjustments will be agreed in advance, documented, and reviewed regularly.

## **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
- 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.





## **Work devices must be used solely for work activities during Directed Time.**

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

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

Where a pupil misuses the school's IT 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 incident.

Where a staff member misuses the school's IT 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 radicalisation.

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 about 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 two years 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 policy
- Staff Disciplinary Procedures
- Data Protection Policy
- Privacy Notice for Pupils, Parents & Carers
- Privacy Notice for Staff & Volunteers
- Complaints Procedures

## **Arrangements for Monitoring and Evaluation**

This policy will be reviewed every two years by the Headteacher and may be amended as appropriate.

Any questions or concerns regarding this policy should be made to:

**Name:** Mr Harry Larter  
**Role:** Computing Subject Lead

**Approved by:**  
**Name:** Elizabeth Hindmarsh  
**Role:** Headteacher  
**Date:** January 2026  
**Date of next review:** January 2028

