E- SAFETY POLICY

2024-25

Contents

Appendix 1: online safety incident report log

Introduction

At St Anne's, we are committed to a high-quality delivery of ICT to enhance and enrich teaching and learning and to educate our pupils about the benefits and risks of using new technology. It is the duty of St Anne's to provide safeguards and awareness for users to enable them to control their online experiences and ensure that they are armed with the knowledge to stay safe in the digital world as well as the physical world.

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

ICT use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction.
Many pupils will access the internet outside school and will need to learn how to evaluate online information and to take care of their own safety and security

This policy document is drawn up to protect pupils, staff, governors and the school community and aims to provide clear advice and guidance on how to minimise risks associated with being online!

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
- Our school will offer a supportive environment where children, staff, parents/carers and governors feel valued, respected and happy.

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and the 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 Body
The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Governing Body will coordinate 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
- Uphold this policy

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
At St Anne's, the overall responsibility for Child Protection and E-Safety lies with the Headteacher, however, a team of Designated Safeguarding Leads support this.

Safeguarding is a serious matter; at St Anne's we use technology and the internet across all areas of the curriculum and ensure that it is comprehensive, age-related and effective.

Online safeguarding, known as E-Safety, is an area that is constantly evolving.

At St Anne's, we ensure that staff E-Safety CPD is current and included in staff induction; as such this policy will be reviewed on an annual basis or in response to an E-Safety incident, whichever is sooner.

Details of the school's Designated Safeguarding Leads (DSL) 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, Computing Lead 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 cyberbullying 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 body

This list is not intended to be exhaustive.

The Computing Lead
The Computing Lead, alongside the IT Technician, is responsible for:
- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a 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 (see Appendix 1) 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
- Working with the DSL to ensure that any online safety incidents are logged

(see Appendix 1) 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/Carers
Anyone not following the rules for E-Safety will be dealt with in line with our behaviour policy.

Parents/carers are expected to:
- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (Appendix 1)

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: https://www.saferinternet.org.uk/advicecentre/parents/carers-andcarers/whatar e-   issues
- Hot   topics, Childnet   International: http://www.childnet.com/parents/carers-and-carers/hottopics

- Parent factsheet,   Childnet International:
http://www.childnet.com/ufiles/parents/carersfactsheet-09-17.pdf

Digital Images
Parents/carers are required to give their consent via ParentMail, our school administration system, for the use of images of their children for school purposes and on the internet: the school website, social media etc - the child's full name is never included with their image. Digital images may be shared with partner schools and organisations as part of collaborative learning projects. All such use is monitored and supervised by staff.

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, addressed primarily through Computing and PSHE teaching and learning as well as other opportunities across 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, where relevant. The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online

Email Safety

We do not allow pupils to send emails externally.

Via the Computing curriculum, they are taught how to use email safely and how to communicate appropriately through email. Staff use the Office 365 email system, and this should only be used for school purposes.

Educating parents/carers about online safety

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

Online safety will also be highlighted during parents' evenings.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher.

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 cyberbullying with their class, and the issue will be addressed in assemblies.

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.

Acceptable use of the internet in school

Pupils' Access to the Internet and Network Safety

All users log on to the network using a year group username and can save and retrieve work stored in a personal folder in their name. On the network, there are different areas where groups of users can save work so that it is available to others. Pupils are taught how to access and save to shared resource areas. Teachers sometimes use the network to share files with each other; children do not have access to these files.

When using networked equipment, all access to the Internet is protected by a number of different filters. These filters are designed to prevent accidental or deliberate access to unsuitable materials. In addition, the network administrators can manually block site addresses which are considered to be unacceptable.

However, no system is 100% safe, and pupils are taught that the Internet contains many websites that are useful but that there are also websites that are unpleasant, offensive or which introduce software which can damage the equipment.

No-one must attempt to access a website that they know to be unsuitable for children and/or containing offensive language, images, games or other media.

At St Anne's, we have an E-Safety curriculum, integrated into our Computing curriculum, which has been designed to teach the children how to keep themselves safe whilst using the internet. We also cover this issue annually during our Anti-Bullying week and regular assemblies. Pupils accessing the Internet at home are subject to the controls placed upon them by their parents/carers.

To support parents/carers in safeguarding their children, on the school website we publish specific advice for parents/carers with regards to ESafety and how best to protect their child in this respect. We also share this advice via newsletters on a regular basis. However, any home use of the Internet made in connection with the school or school activities will be subject to this policy and any breach dealt with as if the event took place at school.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. More information is set out in the acceptable use agreements in appendices and 2.

Pupils using mobile devices in school

Pupils are not allowed mobile phones or personal electronic devices in school - any such items brought in must be handed to the main office/class teacher and then collected at the end of the day.

Mobile devices belonging to staff should not be used to store children's personal data. No personal data such as home addresses, contact telephone numbers, medical information or photographs should be kept on such devices. Mobile phones and personal devices should not be used in teaching areas. Any use of mobile devices in school by pupils must be authorised by a member of staff. 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. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the Computing Lead/ IT Technician.

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. The Headteacher / Designated Safeguarding Leads/ Computing Lead will ensure these procedures are followed by staff in the event of any misuse of the internet: An inappropriate website is accessed inadvertently:

- Report website address to the Computing Lead by logging the incident on the form on Appendix 1.
- The Computing Lead then contacts ICT Technical Support to emend school filters as necessary. An inappropriate website is accessed deliberately:
- Report website address to the Computing Lead by logging the incident on the form on Appendix 1.
- The Computing Lead then contacts ICT Technical Support to amend school filters as necessary.
- Decide on appropriate action. An adult receives inappropriate material:
- Do not forward this material to anyone else.
- Report to the Computing Lead by logging the incident on the form on Appendix 1.
- Contact relevant authorities for further advice e.g. police, social care, CEOP. An illegal website is accessed, or illegal material or evidence of illegal activity is found on a computer: This may contain racist, obscene or violent materials.

If any of the above are found, the following should occur:

- Alert the Headteacher / Computing Lead immediately.
- DO NOT LOG OFF the device, but do bring it to be kept in a safe place.
- Contact the police / CEOP and social care immediately.

- If a member of staff or volunteer is involved, refer to the Disciplinary Policy and report to the Local Authority Designated Officer. Threatening or malicious comments are posted to the school's digital community- Class Dojo-about an adult or child in school, or in the instance that malicious text messages are sent to another child/young person (cyber bullying):
- Preserve any evidence and log the incident using Appendix 4.
- Inform the Headteacher immediately and follow Child Protection Policy.
- Inform a Designated Safeguarding Lead.
- Check the filter if an internet-based website issue.
- Contact/parents/carers and carers.
- Contact the police or CEOP if appropriate.

Training

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, ebulletins and staff meetings).

The DSL undertakes 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.

Monitoring arrangements

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

This policy will be reviewed every 2 years by the Headteacher. At every review, the policy will be shared with the governing body.

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
- Remote Learning Plan and Policy

Remote/Home Learning

We will endeavour to ensure that pupils continue to receive a good level of education 'beyond the classroom' in the circumstance of a class/whole school having to isolate by providing a range of resources via our website and Microsoft Teams.

We expect pupils to follow the same principles, as outlined in the school's Acceptable User policy, whilst learning at home. Pupils must uphold the same level of behavioural expectations as they would in a normal classroom setting. Any significant behavioural issues occurring on any virtual platform must be recorded, reported and appropriate sanction imposed. For all minor behavioural incidents, these should be addressed using the normal restorative approaches. Staff should be mindful that when dealing with any behavioural incidents online, opportunities to discuss and repair harm will not be the same as if the child or young person was in school. Therefore, it may be necessary to have a discussion with the parents/carers, regardless of how minor the incident, to ensure the child is emotionally well supported.

Appendix 1:

St Anne's Roman Catholic Primary School

Online Safety Incident Report Log

Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

15

This policy was approved by the Full Governing Board on 6 December 2023