

St Anne's Catholic Primary School



Online and E Safety policy

Headteacher and Designated Safeguarding Lead: Mrs Rachel Crolla

Chair of Governors and Named Safeguarding Governor: Mrs Carmel Foster

Approved by: The Headteacher and Governing Body **Date:**

Last reviewed: September 2019

Next review due by: September 2020

Contents

1. Aims.....	2
2. Legislation and guidance	3
3. Roles and responsibilities	3
4. Educating pupils about online safety	4
5. Educating parents about online safety	5
6. Cyber-bullying.....	5
7. Acceptable use of the internet in school.....	6
8. Pupils using mobile devices in school	6
9. Staff using work devices outside school.....	6
10. How the school will respond to issues of misuse.....	6
11. Training.....	7
12. Monitoring arrangements	7
13. Links with other policies	7
Appendix 1: acceptable use agreement (pupils and parents/carers)	8
Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)	Error! Bookmark not defined.
Appendix 3: online safety training needs – self-audit for staff.....	10
Appendix 4: online safety incident report log.....	Error! Bookmark not defined.

.....

1. Aims

St Anne's Catholic Primary 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

2. Legislation and guidance

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

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

The policy also takes into account the [National Curriculum Computing programmes of study](#).

3. Roles and responsibilities

3.1 The governing body:

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

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL). (CPOMS Reporting System)

The governor who oversees online safety is Mrs Carmel Foster (Chair)

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)

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

Details of the school's designated safeguarding lead (DSL) (and deputy DSLs) are set out in our Safeguarding and Child Protection Policy.

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

- Ensuring that all staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Deputy Safeguarding Lead, ICT Manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (CPOMS) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged (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.

3.4 The ICT Manager

The ICT manager 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 regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files (Smooth Wall Filtering System).
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy. (Smooth Wall Filtering System).
- 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.

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 (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 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>

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, 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).

4. Educating pupils about online safety

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

In **Key Stage 1**, pupils will be taught to:

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

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly

- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and who to contact should this occur.

5. Educating parents about online safety

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

Information regarding Online Safety will also be shared 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 Class Teacher who will then discuss with the Headteacher (DSL) or the Deputy DSLs. If considered necessary then concerns should be raised directly with the Headteacher (DSL) or the Deputy DSLs.

Concerns or queries about this policy can be raised with any member of school staff.

6. Cyber-bullying

6.1 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.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes and groups, and the issue will be addressed in assemblies as and when necessary, in line with the curriculum.

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.

The school will raise awareness of cyber-bullying to parents through communication, via the school website and links to information, 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 (Headteacher and in the absence of the Headteacher the Deputy Headteacher and /or the Deputy DSLs) 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.

6.3 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.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. St Anne's Catholic Primary School uses the Smoothwall web filtering system in accordance with the LA service Level agreement.

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

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, for the purposes of safety. All phones brought into school must be made known to the class teacher and handed in for supervision until home time. Mobile phones are not permitted to be used during the school day. This includes the hours of After School Club and after school sports clubs/activities, 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.

The term 'mobile device' includes: tablets, smart watches, Kindles or any other electronic device.

9. 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 the Acceptable use of ICT Policy.

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 ICT manager.

Work devices must be used solely for work activities.

10. 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.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

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

The DSL (The Headteacher and therefore in the Headteacher's absence the Deputy Headteacher) (and the Deputy Designated Safeguarding Leads) 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.

12. Monitoring arrangements

The DSLs log behaviour and safeguarding issues related to online safety. This will be done via the Smooth Wall reporting system in accordance with the St Helens Council Service Level Agreement.. This policy will be reviewed each academic year by the Headteacher and Governing Body.

13. Links with other policies/Statements

This online safety policy is linked to our:

- Safeguarding and Child Protection Policy
- Behaviour policy and School Behaviour Charters
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable Use of ICT Policy
- School Social Media Statement

Appendix 1: acceptable use agreement (pupils and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school's ICT systems and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- It will be with my parent's knowledge and permission.
- I will make it known immediately to my class teacher, that I have an electronic device or phone in school and the reason why.
- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- IWhen I do use my device, I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

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

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. I understand that the school uses Smooth Wall web filtering and all material and searches made by my child will be monitored and reported upon for school safeguarding purposes.

Signed (parent/carer):

Date:

Appendix 2: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	Date:
I know the name of the person/people with lead responsibility for Safeguarding – including online safety in school?	
I am aware of what I must do if a pupil approaches me with a concern or issue. This includes use of the School's CPOMS reporting procedures and Safeguarding procedures.	
I am familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors.	
I am familiar with the school's acceptable use agreement for pupils and parents	
I regularly change my password for accessing the school's ICT systems	
I am familiar with St Anne's Catholic Primary school's approach to tackling cyber-bullying should it occur.	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Policy ratified and adopted by the Governing Body on
Signed Headteacher : Mrs Rachel Crolla
Signed Chair of Governors: Mrs Carmel Foster:

