St Charles Catholic Primary School
Online Safety Policy

This Policy was adopted by The Governing Body of St Charles Catholic Primary School on:	
Date: March 2023	**Signed by: L.Powell** Elizabeth L. Powell.
It will be reviewed on: March 2025	

Mission Statement

"Let all that you do be done in Love.
Love is made possible with respect." St Charles Borromeo

At St Charles' we pray, love and learn together as one school family, with Christ at our centre. We create and experience joy every day in our home, our school and our parish.

Vision

Children will leave St. Charles':

- With a love for learning.
- With Christ in their hearts.
- With outstanding manners.
- Showing care and respect for all.
- Having achieved their best.
- With a sense of pride and confidence.
- With a deep sense of responsibility.
- With life-long skills to enhance their future.

Values:

Everyone at St. Charles' will be:

- Compassionate
- Aspirational
- Determined
- Enthusiastic
- Humble
- Friendly
- Trustworthy

Aims

St Charles 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

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 takes into account the National Curriculum computing programmes of study and the Statutory Guidance in 'Relationships Education, Relationships and Sex Education (RSE) and Health Education' DfE 2019.

Roles and responsibilities:

The Local Governing Body

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

The Headteachers termly report to governors will include reference to any online safety incidents.

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

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, on our school website, and displayed around the school site.

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, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMS 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 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 board

The ICT manager (St Thomas Aquinas CMAT)

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
- 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 cyber-bullying are dealt with appropriately in line with the school behaviour policy

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 Staff Code of Conduct and guidance 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 through CPOMS 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

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)

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.

Educating pupils about online safety

Pupils will be taught about online safety as part of the Personal Development and Computing Curriculum.

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

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

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

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

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

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Educating parents about online safety

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

Online safety will also be covered during parents' evenings.

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

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

Cyber-bullying

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 cyber bullying with their tutor groups, 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.

The school also sends information / leaflets on cyber bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to specific incident of cyber bullying, the school will follow the process set out in the school behaviour policy. Where illegal, in appropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident in 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 deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or

- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

Acceptable use of the internet in school

Use of the schools internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individuals role.

Pupils using mobile devices in school

We recognise that mobile phones are part of everyday life for many children and that they can play an important role in helping pupils to feel safe and secure. However, we also know that they can prove a distraction in school and can provide a means of bullying or intimidating others. Therefore:

Pupils are not permitted to have mobile phones at school or on trips. If in the rare event of a parent wishing for his/her child to bring a mobile phone to school to contact the parent after school:

- The phone must be handed in, switched off, to the office first thing in the morning and collected from them by the child at home time (Any phone is left at the owner's own risk)
- Mobile phones brought to school without permission will be confiscated and returned at the end of the day
- Where mobile phones are used in or out of school to bully or intimidate others, then the Headteacher does have the power to intervene 'to such an extent as it is reasonable to regulate the behaviour of pupils when they are off the school site'

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 Trust Central Team.

Work devices must be used solely for work activities.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

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

All staff members will receive refresher training 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 and deputies 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.

Monitoring arrangements
The DSL logs behaviour and safeguarding issues related to online safety.
This policy will be reviewed every 2 years by the Headteacher. At every review, the policy will be shared with the governing board.

Links with other policies
This online safety policy is linked to our:

- Child protection and safeguarding policy
- Staff code of conduct
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

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:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree 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.

Signed (parent/carer):	**Date:**

Appendix 2: Staff and Volunteer Acceptable Use

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion and promote creativity, promoting effective learning. They also bring opportunities for staff to be more creative and productive in their work.

It is intended to ensure:

- that staff and volunteers will be safe and responsible users of the internet and other digital technologies.
- that school ICT systems and users are protected from accidental or deliberate misuse.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work and improve opportunities for learners and will, in return, expect staff and volunteers to agree to be responsible users.

School ICT systems must be used in a responsible way, to minimise the risk to staff safety or to the safety and security of the ICT systems and other users. Staff will, where possible, educate the young people in the safe use of ICT and embed e-safety work with young people.

For staff professional and personal safety:

- The school will monitor staff use of its ICT systems including email and other digital communications technologies (including the use of school ICT systems out of school (eg. laptops, email, VLE etc).
- The school ICT systems are primarily intended for educational use and that staff will only use the systems for personal or recreational use within the policies and rules set down by the school.
- Usernames and passwords are to be kept private ;other people’s username and password will not be used.
- Any illegal, inappropriate or harmful material or incident will be immediately reported to the appropriate person in school.
- Staff will be professional in communications and actions when using school ICT systems.
- Staff will not access, copy, delete or otherwise alter any other user's files, without their permission.
- Taking or publishing images of pupils or parents/colleagues, is only done with their permission and in accordance with the school's policy.
- Personal equipment will not be used to record these images, unless I have permission to do so.
- Where these images are published (eg on the school website) it will not be possible to identify pupils by name, or other personal information.

- Communication with pupils and parents / carers is only done through official school systems and in a professional manner.
- Personal information will not be shared with a pupil (including personal phone numbers or email address). Staff will not request or respond to any personal information from a young person unless it is appropriate as part of their professional role.
- Staff will not engage in any on-line activity that may compromise their professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies:

- When using personal hand held / external devices in school (PDAs / laptops / mobile phones / USB devices etc), staff will follow the rules set out in this guidance in the same way as if using school equipment.
- Personal email addresses are not to be used on the school ICT systems.
- Any attachments to emails are not to be opened unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- Any material which is illegal or inappropriate or may cause harm or distress to others (eg child sexual abuse images, criminally racist material, adult pornography etc) will not be uploaded, downloaded or accessed. Programmes or software that might allow the bypass /filtering of security systems intended to prevent access to such materials will not be used.
- Unless given permission, large downloads or uploads that might take up internet capacity will not be used, as they may prevent other users from being able to carry out their work.
- School equipment must not be damaged or disabled.
- Transporting, holding, disclosing or sharing personal information must be as outlined in the School Data Protection Policy. Where personal data is electronically transferred outside the secure school network, it must be encrypted.
- Damage or faults involving equipment or software, however this may have happened, must be immediately reported.

When using the internet in my professional capacity or for school sanctioned personal use, staff must ensure that they have permission to use the original work of others
Where work is protected by copyright, it will not be download or distributed (including music and videos).