St Edward's Catholic First School
Parsonage Lane, Windsor SL4 5EN
Head Teacher : Mrs Sarah Matthews
Telephone : 01753 860607
office@secfs.org.uk
www.stedwardscatholicfirstschool.co.uk

We See Jesus In Everything We Do

St Edward's Catholic first School

On-Line safety Policy

September 2023

Contents

- **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, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key Categories of Risk

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

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and seminudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance,

Keeping Children Safe in Education 2023, 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 and sex education
- Searching, screening and confiscation

It also refers to the DfE'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 Board

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

The governor who oversees online safety is Dave Roberts.

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 3)

Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures

Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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.

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 dealt with appropriately in line with the school behaviour policy

- 3.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) Sarah Matthews and deputies Andy McKell, Liam Keohane and Imogen Adams are set out in our child protection and safeguarding policy as well as relevant job descriptions.

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

Ensuring that staff understand this policy and that it is being implemented consistently throughout the school

Working with the ICT leader 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 child protection policy

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 4 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

This list is not intended to be exhaustive.

- 3.4 The ICT Leader

The ICT support provider (Cybersupport) is responsible for:

Working with the school's computer team, and ensuring that an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

Ensuring that regular full security checks are carried out and that there is and monitoring of 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

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 (appx 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)

Working with the DSL to ensure 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 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'

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 (appendices 1 and 2)

Parents 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 International
- Parent resource sheet – Childnet International

- 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 3).

4. Educating Pupils about Online Safety

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

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

Relationships education and health education in primary schools

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

By the end of primary school, pupils will know:

That people sometimes behave differently online, including by pretending to be someone they are not.

That the same principles apply to online relationships as to face-to-face relationships, including the

importance of respect for others online including when we are anonymous

The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

How information and data is shared and used online

What sorts of boundaries are appropriate in friendships with peers and others (including in a digital

context)

How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

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.

5. Educating Parents about Online Safety

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

Online safety will also be covered during parents' evenings.

The school will let parents 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 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.

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 1 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.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. 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 and anti-bullying 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6. 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 to 3). 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.

More information is set out in the acceptable use agreements in appendices 1 to 3.

7. Pupils using mobile devices in school

Pupils are not permitted to bring any electronic devices to school.

8. Staff using Work Devices Outside School

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)

Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device

Making sure the device locks if left inactive for a period of time

Not sharing the device among family or friends

Installing anti-virus and anti-spyware software

Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from Cybersupport.

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 our positive 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 relevant policies. 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).

By way of 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

Children can abuse their peers online through:

- Abusive, 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
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

• 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 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.

12. Monitoring arrangements

Behaviour and safeguarding incidents related to online safety will be recorded on CPOMS by staff and responded to and monitored by a member of the Safeguarding Team.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Anti-bullying policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: EYFS & KS1 Acceptable Use Agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET AGREEMENT FOR EYFS & KS1 (Year 1&2) PARENTS/CARERS	
Pupil Name:	Class:
Parents must be aware that the school uses computers and tablets to teach the children skills and safety. The below is a list of the dangers we will teach them to look out for as part of the curriculum. Please sign below to confirm that you consent for the children to undertake these lessons and that you will reinforce these principles at home. Children will; • Ask a teacher or adult if they can do so before using them • Only use websites that a teacher or adult has told them about or allowed them to use • Tell the teacher immediately if they: • Click on a website by mistake • Receive messages from people I don't know • Find anything that may upset or harm me or my friends They will also, • Use school computers for school work only • Be kind to others and not upset or be rude to them • Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly • Only use the username and password they have been given • Try their hardest to remember their username and password • Never share their password with anyone, including my friends. • Never give personal information (name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer • Save all work on the school network • Check with their teacher before printing anything • Log off or shut down a computer when they have finished using it I agree that the school will monitor the websites the children visit and that there may be consequences if they do not follow the rules.	
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 will make sure my child understands these.	
Signed (Parent)	Date

Appendix 2: KS2, Acceptable Use Agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR KS2 (Year 3 & 4) PUPILS AND PARENTS/CARERS	
Pupil Name:	Class:
I will read and follow the rules in the acceptable use agreement policy. When I use the school's ICT systems (like computers) and get onto the internet in school I will: • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission	

• Keep my usernames and passwords safe and not share these with others
• Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
• Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
• Always log off or shut down a computer when I've finished working on it

I will not:

• Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
• 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
• Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
• Log in to the school's network using someone else's details
• Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

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 will make sure my child understands these.

Signed (Parent)	Date

Appendix 3: Acceptable Use Agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR Staff, Governors, Volunteers & Visitors	
Name:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first and only using school equipment • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed	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 will make sure my child understands these.	
Signed (Parent)	Date

Appendix 4 – Online Safety Training Audit

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name	
Question	**Answer – Yes/No**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Reviewed:	Headteacher	September 2023
Approved:	FGB	19th September 2023
Ratified:	FGB	19th September 2023
Review frequency	Annually	