



English Martyrs Catholic Primary School

*"where everyone is special"*

## P57: Online Safety Policy

### Mission Statement

With Christ at the heart of our Catholic community,  
our mission is to:

- ✘ nurture the potential in each individual,
- ✘ celebrate achievement,
- ✘ and develop an awareness of service  
to God and each other

**Adopted by the school: October 2021**

**Review: When required**

## Contents

1. Aims .....	3
2. Legislation and guidance .....	3
3. Roles and responsibilities .....	3
4. Educating pupils about online safety .....	5
5. Educating parents about online safety .....	6
6. Cyber-bullying .....	6
7. Acceptable use of the internet in school .....	7
8. Pupils using mobile devices in school .....	7
9. Staff using work devices outside school .....	7
10. How the school will respond to issues of misuse .....	8
11. Training .....	8
12. Monitoring arrangements .....	9
13. Links with other policies .....	9
Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers) .....	10
Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers) .....	11
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors) .....	14
Appendix 4: online safety training needs – self audit for staff .....	15
Appendix 5: online safety incident report log .....	16

---

## 1. 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, anti-Semitism, 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 semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- › **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

## 2. Legislation and guidance

This policy is based on the Department for Education's (DfE) 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 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 governing board 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).

The governor who oversees online safety is Siobhan Loydall (Foundation Governor)

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, 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.

### **3.3 The designated safeguarding lead**

Details of the school's DSL and Deputy DSL 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:

- › Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- › Working with the headteacher, Online Safety Lead 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 (see appendix 5) 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 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 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 (see appendix 5) 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.

### **3.5 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](#)
- › Healthy relationships – [Disrespect Nobody](#)

### 3.6 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

**All schools**

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 letters 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.

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 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.

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).

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 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.

### **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\*

\* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- › The DfE's latest guidance on [screening, searching and confiscation](#)
- › UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- › The school's COVID-19 risk assessment

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 1-3). 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, 2 and 3.

## 8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during the school day. They are to be kept safely in the school office.

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.

## 9. 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 – always install 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 Computing Subject Leader or Headteacher.

## 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 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 code of conduct. 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 the risks up
- 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 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 DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Online Safety Leader. At every review, the policy will be shared with the governing board. 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.

## **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 and privacy notices
- Complaints procedure



## Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)



### English Martyrs Catholic Primary School

*"where everyone is special"*

#### Pupil Acceptable Use Policy Agreement for Younger Children

**This is how we stay safe when we use computers:**

- I will ask a teacher or suitable adult if I want to use the computers / iPads
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I will not search for things on the internet that I have not been asked to do
- I will not use my own phone, ipad or other personal systems in school or at any school related events
- I know that if I break the rules I might not be allowed to use a computer / iPad

Signed (child): .....

Signed (teacher): .....

Date: .....



## Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)



# English Martyrs Catholic Primary School

*"where everyone is special"*

## Pupil Acceptable Use Policy Agreement

(Year 3 to Year 6)

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

### **For my own personal safety:**

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure - I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, etc )
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

### **I understand that everyone has equal rights to use technology as a resource and:**

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

**I will act as I expect others to act toward me:**

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

**I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school / academy:**

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed

**When using the internet for research or recreation, I recognise that:**

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

**I understand that I am responsible for my actions, both in and out of school:**

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

-----  
-----

## Pupil Acceptable Use Agreement Form (Key Stage Two)

This form relates to the Pupil Acceptable Use Policy Agreement.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school).
- I use my own equipment out of the school in a way that is related to me being a member of this school eg communicating with other members of the school, accessing school email, VLE, website etc.
- I **do not** use my own devices in the school or school related events at any time eg mobile phones, gaming devices USB devices, cameras at any time, including school related events eg discos, fetes etc.
- Any breach in the user agreement will be dealt with severely and appropriately by the school.

Name of Student / Pupil: .....

Class: .....

Signed: .....

Date: March 2018

## 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 AND VISITORS

**Name of staff member/governor/volunteer/visitor:**

**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
- 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 (staff member/governor/volunteer/visitor):**

**Date:**

## Appendix 4: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
<b>Name of staff member/volunteer:</b>	<b>Date:</b>
Question	Yes/No (add comments if necessary)
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?	



## Appendix 5: online safety incident report log

# English Martyrs Catholic Primary School

*"where everyone is special"*



## ICT Incident Report Form

This form should be filled out if a child breaches the Pupil User Agreement.

Name of Pupil:	Year Group: R, 1, 2, 3, 4, 5, 6
Description of incident	
Technology used:	
Actions taken:	
Name of person completing this form	Date and time of incident reported:
Action taken by management (if appropriate)	
Duration of exclusion from ICT technology:	
Online Safety Lead informed: Y/N	Parents informed: Y/N
Signed:	Date: