St. Joseph's Catholic Primary School

Online Safety Policy

Policy	Online Safety Policy
Date Agreed	May 2024
Date of Next Review	May 2025
Governor Signature	G. Spencer
Executive Headteacher Signature	M. Corcoran

1. Introduction

Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks.

We want to equip our pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world.

2. 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 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 scams

3. Roles and responsibilities

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 make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Governing Board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards.

This list is not intended to be exhaustive.

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 (DSL)

Details of the school's Designated Safeguarding Lead DSL is 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 and Governing Board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly

Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.

This list is not intended to be exhaustive.

The ICT Manager

The ICT Manager is responsible for:

Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually 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

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 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

This list is not intended to be exhaustive.

All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

Maintaining an understanding of this policy

Implementing this policy consistently

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)

Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by emailing the DSL & the ICT Manager.

Following the correct procedures by contacting Elementary if they need to bypass the filtering and monitoring systems for educational purposes

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.

Parents/Carers

Parents/carers are expected to:

Notify a member of staff or the Headteacher of any concerns or queries regarding this policy

Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.

4. Curriculum Context

As part of the relationships and health education in primary our pupils are taught about online safety and harms. This includes being taught:

- what positive, healthy and respectful online relationships look like
- the effects of their online actions on others
- how to recognise and display respectful behaviour online

Throughout these subjects, we address online safety and appropriate behaviour in an age-appropriate way that is relevant to pupils' lives.

This complements the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes:

- how to use technology safely, responsibly, respectfully and securely
- where to go for help and support when they have concerns about content or contact on the internet or other online technologies

There are also other curriculum subjects which include content relevant to teaching pupils how to use the internet safely. For example, citizenship education explores:

- freedom of speech
- the role and responsibility of the media in informing and shaping public opinion
- the concept of democracy, freedom, rights, and responsibilities

5.Underpinning Knowledge and Behaviours

The online world develops and changes at a great speed. New opportunities, challenges and risks are appearing all the time. This can make it difficult for schools to stay up to date with the latest devices, platforms, apps, trends and related threats.

It is important that we focus on the underpinning knowledge and behaviours that can help our pupils to navigate the online world safely and confidently regardless of the device, platform or app. This teaching is:

- built into existing lessons across the curriculum
- covered within specific online safety lessons
- covered using school-wide approaches

Teaching is always age and developmentally appropriate

How to Evaluate What Pupils See Online

Covering this content will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

You can help pupils to consider:

- whether a website, URL or email is fake
- what cookies do and what information they are sharing
- if a person or organisation is who they say they are
- why a person wants them to see, send or believe something
- why a person wants their personal information
- the reason why something has been posted
- whether something they see online is fact or opinion

How to Recognise Techniques Used for Persuasion

Covering this content will enable our pupils to recognise the techniques that are often used to persuade or manipulate others.

You can help pupils to recognise:

- online content which tries to make people believe something false is true or mislead (misinformation and disinformation)
- techniques that companies use to persuade people to buy something
- ways in which criminals may try to defraud people online
- ways in which games and social media companies try to keep users online longer (persuasive or sticky design)
- grooming and manipulation techniques used by criminals
- ways to protect themselves from a range of cyber crime

Online Behaviour

Covering this content enables pupils to understand what acceptable and unacceptable online behaviour look like. We teach pupils:

- that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others
- to recognise unacceptable behaviour in others

We help pupils to recognise acceptable and unacceptable behaviour by:

- looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do
- looking at how online emotions can be intensified resulting in mob mentality
- looking at the key principles behind a constructive discussion, including a willingness to listen to other opinions and a readiness to be educated on a topic
- considering how to demonstrate empathy towards others (on and offline)
- teaching techniques (relevant on and offline) to defuse or calm arguments, for example, a disagreement with friends, and disengage from unwanted contact or content online
- considering unacceptable online behaviours often passed off as so-called social norms or just banter, for example, negative language being used as part of online gaming but would never be tolerated offline

How to Identify Online Risks

Covering this content will enable our pupils to identify possible online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online. The focus should be to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

We help pupils to identify and manage risk by discussing:

- the ways in which someone may put themselves at risk online
- risks posed by another person's online behaviour
- when risk taking can be positive and negative

- online reputation and the positive and negative aspects of an online digital footprint
- sharing information online and how to make a judgement about when and how to share and who to share with
- the risks of cyber-crime, online fraud and identity theft

Artificial Intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

St Joseph's recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

We will treat any use of AI to bully pupils in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

How and When to Seek Support

Through this aspect of learning we enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

We help pupils by explaining how to:

- identify who trusted adults are
- access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations such as Childline and Internet Watch Foundation
- report cyber-crime, fraud and suspicious online activity, through organisations such as Action Fraud and the Advertising Standards Authority
- report inappropriate contact or content for various platforms and apps

We link this to wider school policies and processes around reporting of safeguarding and child protection incidents and concerns to school staff. Refer to Keeping Children Safe in Education for more information

6.Teaching about Harms and Risks

Understanding and applying knowledge and behaviours provides our pupils with a solid foundation to navigate the online world in an effective and safe way. By understanding the risks that exist online.

Age Restrictions

Some online activities have age restrictions because they include content which is not appropriate for children under a specific age.

Teaching includes:

- explaining that age verification exists and why some sites require a user to verify their age, for example, online gambling and purchasing of certain age restricted materials such as alcohol
- explaining why age restrictions exist, for example, they provide a warning that the site may contain disturbing material that is unsuitable for younger viewers
- helping pupils understand how this content can be damaging to under-age consumers
- explaining what the age of digital consent means - the minimum age (13) at which young people can agree to share information and sign up to social media without parental consent under General Data Protection Regulations

We cover this content in the following curriculum areas:

- health education (all stages) - internet safety and harms topic
- computing (all key stages) – you may want to discuss age restrictions as part of e-safety
- citizenship (key stage 2)

How Content can be Used and Shared

Knowing what happens to information, comments or images that are put online.

Teaching includes aspects such as:

- what a digital footprint is, how it develops and how it can affect future prospects such as university and job applications
- how cookies work
- how content can be shared, tagged and traced
- how difficult it is to remove something a user wishes they had not shared
- the risk of identity theft or targeted approach from fraudsters using information shared online
- ensuring pupils understand what is illegal online, for example:
    - youth-produced sexual imagery (sexting)
    - sharing illegal content such as extreme pornography or terrorist content

- the illegality of possession, creating or sharing any explicit images of a child even if created by a child

We cover this content in the following curriculum areas:

- relationships education core content (all stages) – online relationships topic
- health education core content (all stages) – internet safety and harms topic
- computing (all key stages)
- citizenship – (key stage 2)

Disinformation, Misinformation, Malinformation and Hoaxes

Some information shared online is accidentally or intentionally wrong, misleading, or exaggerated.

Teaching includes aspects such as:

- disinformation and why individuals or groups choose to share false information in order to deliberately deceive
- misinformation and being aware that false and misleading information can be shared inadvertently
- malinformation and understanding that some genuine information can be published with the deliberate intent to harm, for example releasing private information or photographs (including revenge porn)
- online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons
- explaining that the viral nature of this sort of content can often appear to be a stamp of authenticity and therefore why it is important to evaluate what is seen online
- how to measure and check authenticity online
- the potential consequences of sharing information that may not be true

We cover related content in the following curriculum areas:

- relationships education (all stages)
- health education (all stages)
- computing (key stage)
- citizenship (key stage 2)

Fake Websites and Scam Emails

Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or another gain.

Teaching includes aspects such as:

- how to look out for fake URLs and websites

- ensuring pupils understand what secure markings on websites are and how to assess the sources of emails
- explaining the risks of entering information to a website which isn't secure
- what to do if harmed, targeted or groomed as a result of interacting with a fake website or scam email
- who to go to and the range of support that is available
- explaining the risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist

We cover this content in the following curriculum areas:

- relationships education (all stages)
- health education (all stages)
- computing (all key stages)
- citizenship – media and information literacy (key stage 2)

Password Phishing

Password phishing is the process by which people try to find out your passwords so they can access protected content

Teaching includes aspects such as:

- why passwords are important, how to keep them safe and that others may try to trick you to reveal them
- explaining how to recognise phishing scams, for example, those that try to get login credentials and passwords
- the importance of online security to protect against viruses (such as keylogging) that are designed to access, steal or copy passwords
- what to do when a password is compromised or thought to be compromised

Personal Data

Online platforms and search engines gather personal data. This is often referred to as 'harvesting' or 'farming'.

Teaching includes aspects such as:

- how cookies work
- how data is farmed from sources which look neutral, for example, websites that look like games or surveys that can gather lots of data about individuals
- how, and why, personal data is shared by online companies, for example, data being resold for targeted marketing by email and text (spam)
- how pupils can protect themselves, including what to do if something goes wrong (for example data being hacked) and that acting quickly is essential
- the rights children have with regard to their data, including particular protections for children under the General Data Protection Regulations (GDPR)

- how to limit the data companies can gather, including paying particular attention to boxes they tick when playing a game or accessing an app for the first time

We cover related content in the following curriculum areas:

- relationships education core content (all stages) – online relationships topic
- computing (all key stages)
- citizenship – rights and the law (key stage 2)

Persuasive Design

Many devices, apps and games are designed to keep users online for longer than they might have planned or desired.

Teaching includes aspects such as:

- explaining that the majority of games and platforms are businesses designed to make money - their primary driver is to encourage users to be online for as long as possible to encourage them to spend money (sometimes by offering incentives and offers) or generate advertising revenue
- how designers use notifications to pull users back online

We cover related content in the following curriculum areas:

- health education core content (all stages) – internet safety and harms topic
- computing (all key stages)

Privacy Settings

Almost all devices, websites, apps and other online services come with privacy setting that can be used to control what is shared.

Teaching includes aspects such as:

- how to find information about privacy setting on various sites, apps, devices and platforms
- explaining that privacy settings have limitations, for example, they will not prevent someone posting something inappropriate

We cover related content in the following curriculum areas:

- relationships education core content – online relationships topic

- computing (all key stages)

Targeting of Online Content (including on social media and search engines)

Much of the information seen online is a result of some form of targeting.

Teaching includes aspects such as:

- how adverts seen at the top of online searches and social media feeds have often come from companies paying to be on there and different people will see different adverts
- how the targeting is done, for example, software which monitors online behaviour (sites they have visited in the past, people who they are friends with) to target adverts thought to be relevant to the individual user
- the concept of clickbait and how companies can use it to draw people onto their sites and services

We cover related content in the following curriculum areas:

- health education core content (all stages) - internet safety and harms topic
- computing (all key stages)
- citizenship – media and information literacy (key stages 2)

How to Stay Safe Online

This section covers elements of online activity that could adversely affect a pupil's personal safety or the personal safety of others online.

Age-specific advice on these potential harms and risks can be found in the following sections of the education for a connected world framework:

- online relationships
- privacy and security
- online reputation
- online bullying

Abuse (online)

Some online behaviours are abusive. They are negative in nature, potentially harmful and in some cases can be illegal.

Teaching includes aspects such as:

- explaining about the types of online abuse including sexual, harassment, bullying, trolling and intimidation

- explaining when online abuse can cross a line and become illegal, such as forms of hate crime and blackmail
- how to respond to online abuse including how to access help and support
- how to respond when the abuse is anonymous
- discussing the potential implications of online abuse, including the implications for victims
- being clear about what good online behaviours do and don't look like

We cover related content in the following curriculum areas:

- relationships education core content (all stages) – online relationships topic
- health education core content (all stages) – internet safety and harms topic
- computing (all key stages)
- citizenship (key stages 2)

Fake Profiles

Not everyone online is who they say they are.

Teaching includes aspects such as:

- explaining that in some cases profiles may be people posing as someone they are not (such as an adult posing as a child) or may be bots (which are automated software programs designed to create and control fake social media accounts)
- how to look out for fake profiles, for example:
    - profile pictures that don't like right, for example, of a celebrity or object
    - accounts with no followers or thousands of followers
    - a public figure who doesn't have a verified account

We cover related content in the following curriculum areas:

- relationships education core content (all stages) – online relationships topic
- computing (all key stages)

Grooming

Knowing about the different types of grooming and motivations for it, for example:

- radicalisation
- child sexual abuse and exploitation
- gangs (county lines)
- financial exploitation (money mules)

Teaching (at an age-appropriate level) includes aspects such as:

- boundaries in friendships with peers, families and with others
- the key indicators of grooming behaviour
- explaining the importance of disengaging from contact with suspected grooming and telling a trusted adult
- how and where to report it both in school, for safeguarding and personal support, and to the police

See the National Crime Agency's think u know website for further information on keeping children safe from sexual abuse and exploitation.

Well-being

This section covers the elements of online activity that can adversely affect a pupil's well-being.

Age-specific advice on these potential harms and risks can be found in the following sections of the education for a connected world framework:

- self-image and identity
- online reputation
- online bullying
- health, wellbeing and lifestyle

7. Vulnerable Pupils

Any pupil can be vulnerable online, and their vulnerability can fluctuate depending on their age, developmental stage and personal circumstance.

However, there are some pupils, for example, looked after children and those with special educational needs, who may be more susceptible to online harm or have less support from family or friends in staying safe online. You should consider how you tailor your offer to make sure these pupils receive the information and support they need.

The following resources can help schools consider how best to support their most vulnerable pupils stay safe online:

- vulnerable children in a digital world - a report from Internet Matters
- children's online activities, risks and safety - a literature review by the UK Council for Internet Safety's evidence group

8.Use of External Resources

Schools are best placed to make their own decisions about which resources are educationally appropriate for their pupils. This includes reviewing resources, even when from a trusted source, as some will be more appropriate to their cohort of pupils than others.

Before using any resource, you should check:

- where the organisation gets their information from
- what their evidence base is
- if they have been externally quality assured
- the background of the organisation
- if the resources are age appropriate for pupils
- if the resources are appropriate for the developmental stage of pupils

9.Use of External Visitors

Online safety can be a difficult and complex topic which changes very quickly. Therefore, schools may want to seek external support who have expertise, up to date knowledge and information.

The right external visitors can provide a useful and engaging approach to deliver online safety messages, but this should enhance a school's offer rather than be delivered in isolation.

10.Safeguarding

As with any safeguarding lessons or activities, it is important that schools consider the topic they are covering and the potential that a child (or more than one child) in the class may be suffering from online abuse or harm in this way.

It is important to create a safe environment in which pupils feel comfortable to say what they feel. If a pupil thinks they will get into trouble or be judged for talking about something which happened to them online they may be put off reporting it and getting help.

Where schools are already aware of a child who is being abused or harmed online they should carefully plan any lesson to consider this, including not drawing attention to that child in a way that would highlight or publicise the abuse. It is good practice to include the Designated Safeguarding Lead (or a deputy) when planning any safeguarding related lessons or activities (including online). They will be best placed to reflect and advise on any

known safeguarding cases, and how to support any pupils who may be especially impacted by a lesson.

In some cases, a pupil will want to make a disclosure following a lesson or activity. The lesson may have provided the knowledge that enabled the pupils to realise they are being abused or harmed or give them the confidence to say something. This is why it is essential all pupils are clear what the school's reporting mechanisms are.

As per keeping children safe in education your reporting mechanisms should be child friendly and operate with the best interests of the pupil at their heart.

Th school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards.

11.Whole School Approach

Whole school approaches are likely to make teaching more effective than lessons alone. A whole school approach is one that goes beyond teaching to include all aspects of school life, including:

- culture
- ethos
- environment
- partnerships with families and the community

We recommend that schools embed teaching about online safety and harms within a whole school approach.

Incorporating the Principles of Online Safety Across All Elements of School Life

You should reflect the principles of online safety in the school's policies and practice where appropriate, and communicate this with staff, pupils and parents. This could include, for example:

- having clear processes for reporting incidents or concerns in the child protection policy
- reflecting online behaviours in the school's behaviour and bullying policies

Keeping children safe in education provides advice for schools on embedding online safety into their broader safeguarding and child protection approach.

Pupils should be just as clear about what is expected of them online as offline.

12.Educating Parents/Carers About Online Safety

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

Online safety will also be covered during parents' evenings.

The school will let parents/carers 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/carers 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.

Further sources of information

This list provides links to relevant government guidance and a range of national organisations who can offer support.

Related guidance is available on:

- relationships and sex education (RSE) and health education
- national curriculum in England computing programmes of study
- national curriculum in England citizenship programmes of study
- keeping children safe in education
- behaviour in schools

Support and resources are also available from:

- the CEOP Thinkuknow Programme
- the NCA's Click CEOP
- National Centre for Computing Education (NCCE)
- UK Council for Internet Safety
- Education for a Connected World

Schools also get advice from national organisations such as:

- Anti-Bullying Alliance
- Association for Citizenship Teaching
- Childnet
- Internet Matters
- Internet Watch Foundation
- NSPCC learning
- Parent Zone's school resources
- PSHE Association
- UK Safer Internet Centre

Parents can refer to the following national organisations for support:

- Internet Matters
- NSPCC
- Parent Zone

Pupils can refer to the following national organisations for support:

- BBC Own It

Childline