



Saint Edmund's and Saint Thomas' Catholic Primary School

Online-Safety Policy

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- provide staff with the overarching principles that guide our approach to online safety
- ensure that, as a primary school, we operate in line with our values and within the law in terms of how we use online devices.

The policy statement applies to all staff, volunteers, children and young people and anyone involved in activities carried out at St. Edmund's and St. Thomas' Catholic Primary School.

Online Abuse

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England from **Online Abuse**.

Online abuse is any type of abuse that happens on the internet, facilitated through technology like computers, tablets, mobile phones and other internet-enabled devices (Department for Education, 2018; Department of Health, 2017; Scottish Government, 2021; Welsh Assembly Government, 2018).

It can happen anywhere online that allows digital communication, such as:

- social networks
- text messages and messaging apps i.e. What's App and Snapchat
- email and private messaging
- online chats
- comments on live streaming sites i.e. Instagram and Facebook
- voice chat in games.

Children and young people can be re-victimised (experience further abuse) when abusive content is recorded, uploaded or shared by others online. This can happen if the original abuse happened online or offline.

Children and young people may experience several types of abuse online:

- [bullying/cyberbullying](#)
- [emotional abuse](#) (this includes emotional blackmail, for example pressuring children and young people to comply with sexual requests via technology)
- [sexting](#) (pressure or coercion to create sexual images)
- [sexual abuse](#)
- [sexual exploitation](#).

Children and young people can also be groomed online: perpetrators may use online platforms to build a trusting relationship with the child in order to abuse them. This abuse may happen online or the perpetrator may arrange to meet the child in person with the intention of abusing them.

Impact of Online Abuse

Whether abuse happens online or offline it can have a long-lasting impact on a child's overall wellbeing. Online abuse can lead to:

- anxiety
- self-harm
- eating disorders
- suicidal thoughts

(Department for Digital, Culture, Media and Sport (DCMS) and Home Office, 2020).

Cyber-Bullying

Specific examples of cyber-bullying include;

- excluding a child from online games, activities or friendship groups
- sending threatening, upsetting or abusive messages
- creating and sharing embarrassing or malicious images or videos
- 'trolling' - sending menacing or upsetting messages on social networks, chat rooms or online games
- voting for or against someone in an abusive poll
- setting up hate sites or groups about a particular child
- creating fake accounts, hijacking or stealing online identities to embarrass a young person or cause trouble using their name.

Impact of Cyber-Bullying

Research shows that cyberbullying has similar effects to offline bullying. It can lead to:

-falling behind at school

-depression

-anxiety

-other mental health difficulties.

-Cyberbullying can make children feel more frightened and helpless than bullying that happens offline. Contact from cyberbullies can happen at any time, anywhere and this can make children feel like they can't escape (Munro, 2011).

We believe that:

- children and young people should never experience abuse of any kind
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- the online world provides everyone with many opportunities; however it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people safe online, whether or not they are using [name of organisation]'s network and devices
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

As well as providing regular teaching and learning opportunities dedicated to Online Safety within the Computing curriculum and PSHE lessons, we will seek to keep children and young people safe by:

- appointing an online safety coordinator Mrs Metcalfe
- providing clear and specific directions to staff on how to behave online through our Code of Conduct Policy for staff
- supporting and encouraging our children to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- supporting and encouraging parents and carers to do what they can to keep their children safe

- developing an online safety agreement for use with young people and their parents or carers and ensuring that Online Safety newsletters are shared with parents each month (See Appendix A)
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child or young person
- reviewing and updating the security of our information systems regularly
- ensuring that user names, logins, email accounts and passwords are used effectively
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- providing support and training for all staff and on dealing with all forms of abuse, including bullying or cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

Harmful Online Hoaxes

The Designated safeguarding Lead should check the factual basis of any harmful online challenge or online hoax with a known, reliable and trustworthy source, such as the [Professional Online Safety Helpline](#) from the UK Safer Internet Centre. Where harmful online challenges or online hoaxes appear to be local (rather than large scale national ones) local safeguarding advice, such as from the local authority or local police force, may also be appropriate and helpful.

Related policies and procedures

This policy statement is read alongside our school policies and procedures, including:

- child protection
- procedures for responding to concerns about a child or young person's well-being
- dealing with allegations of abuse made against a child or young person

- code of conduct for staff and volunteers
- anti-bullying policy and procedures
- photography and image sharing guides

Links for Parents

- [Parent Info: help and advice for families in a digital world](#)
- [Internet Matters: helping parents keep their children safe online](#)
- [NSPCC: online safety](#)
- [London grid for learning \(LGfL\): online safety](#)
- [UK safer internet centre: Tips, advice, guides and resources to help keep your child safe online](#)
- [Childnet international: parents and carers toolkit](#)
- [Parentzone: experts in digital family life](#)
- [LGfL: parents - scare or prepare](#)
- [Thinkuknow: what to do if there's a viral scare online](#)

References

[Harmful online challenges and online hoaxes'](#) DFE

[Keeping Children Safe in education 2025](#)

Policy Revised June 2026 Review Date June 2029