



CHRIST the KING

Catholic Primary School and Nursery with
The Ark, a Specialist Resource



“Loving Learning Growing together as Christ’s family”

ONLINE SAFETY POLICY

Management of policy

Policy owner	Headteacher
Approval level:	FGB
Date of next review	February 2029
Review cycle	Triennial
Type of Policy:	Non-Statutory
Statutory Guidance	See policy

Statement of Intent

At Christ the King we understand that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout school; therefore, there are a number of controls in place to ensure safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised under four areas of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, misinformation, disinformation, conspiracy theories, 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

Legislation and Guidance

- DfE (2024) 'Filtering and monitoring standards for schools and colleges'
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2025) 'Keeping children safe in education 2025'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

Roles and responsibilities

The governing board is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.

- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The headteacher is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and governing board to update this policy on an annual basis.

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Maintaining detailed, secure and accurate written records of reported online safety concerns as well as the decisions and whether or not referrals have been made.
- Understanding the purpose of record keeping.
- Understanding the filtering and monitoring processes in place at the school
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.

- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Working closely with the police during police investigations.
- Keeping up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.

ICT Consultant is responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- 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.

All staff members are responsible for:

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

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Parents are responsible for:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy.
- Reporting online safety incidents and concerns in line with the procedures within this policy.
- Make sure that their child is monitored while using electronic devices to ensure online safety.

Pupils are responsible for:

- Seeking help from school staff if they are concerned about something they or a peer have experienced online.

- Reporting online safety incidents and concerns in line with the procedures within this policy.

Educating pupils about online safety

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

All schools have to teach:

Relationships education and health education in primary schools

In Key Stage (KS) 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 (KS) 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
- Be discerning in evaluating digital content

By the end of primary school, pupils will know:

- That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- 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, 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 are shared and used online
- How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted
- 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 benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- 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.

Our Online Safety curriculum is taught in various ways:

- In discrete lessons throughout the year
- As an ongoing thread throughout the year
- As part of our PSHE curriculum

Our discrete lessons are based on current best practice.

We continue to hold Online Safety Days as appropriate. These provide age appropriate information about online safety for all pupils and share appropriate information around online safety in our newsletter and on our website for parents. We believe in a collaborative approach in ensuring online safety

How should the school's website content be managed?

- The points of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Website photographs that include pupils will be selected appropriately (as defined in this document). Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

Acceptable use of the internet in school

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 and restrict access through filtering systems where appropriate.

Unacceptable use of the Internet

- Pupils will not be allowed access to public or unregulated chat rooms.
- Pupils will not access any social networking sites unless supervised by staff when posting on the school twitter account.
- Staff should not access social networking sites during hours in the school day when children are present.
- No member of staff should engage in direct communication (in or out of school) of a personal nature with a pupil (who is not a member of their direct family) or a parent about school matters, by any means, for example via SMS text message, email, instant messaging, social networking site or telephone.
- No member of staff should add photos and/or tag other members of staff in photos on social media when conducting school business/or on trips.
- Staff and pupils should not access any website which would normally be deemed to be inappropriate in the setting of a primary school (such as those centred on violence, pornography, adult themes etc).

Personal websites/ blogs and social media

- When electronically publishing material on to websites, via text messaging or elsewhere, all members of the school community should consider the thoughts and feelings of those who might be affected by such action. Material that victimises, bullies or unfairly criticises someone else, or is otherwise offensive, is unacceptable.
- We have a school blog that can be updated by staff and children. Staff need to ensure the content is appropriate.

- Staff should not use blogs, websites or social networking media (such as Facebook or Twitter) etc. to publicly discuss sensitive or confidential school issues.
- Access to social networking sites is filtered as appropriate. Staff and pupils are not permitted to use social media for personal use during lesson time. Staff can use personal social media during break and lunchtimes; however, inappropriate use of personal social media during school hours may result in further action. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.
- Staff receive training on how to use social media safely and responsibly. Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media. Where staff are parents of children in the school and have an existing personal relationship with a parent and thus are connected with them on social media, e.g. they are friends with a parent at the school, they will ensure that their social media conduct relating to that parent is appropriate for their position in the school.
- Concerns regarding the online conduct of any member of the school community on social media both in and out of school hours are reported to the Headteacher/DSL or Chair of Governors if these concerns are about the Headteacher and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behaviour and Disciplinary Policy.
- See Appendix 1

Photographic, video and audio technology

- Care should be taken when capturing photographs or video to ensure that all pupils are appropriately dressed.
- Staff will only use school devices (Ipsads) to photograph pupils in a way which supports and celebrates their education.
- Staff must not use their own mobile phones when they are working directly with pupils. The use of such devices should be restricted to break times and lunch times or after school.

Online training and awareness

- All staff must ensure that they are familiar with, and understand, the indicators that pupils may be unsafe online.
- The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.
- All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.
- The DSL (Designated Safeguarding Lead) has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online.
- The importance of online safety is integrated across the school.
- The school will periodically remind children, staff and parents about how to 'stay safe'

- online, via computing and PHSE lessons, assemblies and through visiting speakers. Children will be made aware of the dangers of talking to strangers online, as well as what online-bullying involves and how to address it.
- Staff receive regular email updates regarding online safety information and any other changes to online safety guidance or legislation.
- If a member of staff becomes aware of a child using the internet inappropriately or in an unsafe way, it will be immediately addressed with that child and if appropriate, their peers. Parents will also be informed so that they can help to address the situation.
- Any concerns about a child using the internet or other electronic media inappropriately, should be reported initially to the head of key stage. Safeguarding concerns should be reported to the schools' designated person(s).

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.

Artificial intelligence (AI)

Generative 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 Gemini.

Christ the King 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.

Our schools will treat any use of AI to bully pupils very seriously, in line with our anti-bullying/behaviour policies.

In school, we will be only using the recommended AI tool, which has been reviewed and approved in line with the Department for Education (DfE) guidance. All other AI tools are blocked on the school network, as they do not comply with the DfE's recommendations for safety, data protection, and responsible use.

Staff are also expected to only use the approved AI tool when preparing school work off-site, to ensure consistency, safeguarding, and compliance with data-handling requirements.

See Safe Use of AI policy for further information

Mental Health

The internet, particularly social media, can be a root cause of a number of mental health issues in pupils, eg. Low self-esteem and suicidal ideation. Staff will be aware that online activity both inside and outside of school can have substantial impact on a pupils' mental health state, both positively and negatively. All concerns should be raised following school policies and procedures.

Educating parents/Carers

The school works in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online is raised with regular updates in the weekly newsletter.

Cyber-bullying

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.)

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 encourage them 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 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.
- The school also sends information/leaflets on cyber-bullying to parents/carers so 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 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.

Filtering and monitoring online activity

- The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
- The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.
- The headteacher/School Business Manager and ICT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. ICT technicians will undertake **monthly** checks on the filtering and monitoring systems to ensure they are effective and appropriate.
- Requests regarding making changes to the filtering system will be directed to the headteacher. Prior to making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes.
- Deliberate breaches of the filtering system will be reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

- If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.
- The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

Maintenance and security of the ICT system

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be updated regularly.
- Staff and pupil laptops/tablets will be stored away safely overnight and pupil laptops/tablets will always be left charging.
- If teachers take their school laptops home, they should take appropriate measures to ensure the security of these.

Use on behalf of the school

The school's official social media channels are only used for official educational or engagement purposes. Staff members must be authorised by the headteacher to access to the school's social media accounts.

All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

The school website

- The headteacher and governors are responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.
- The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils is not published on the website.

Confidentiality

- Personal data and information about staff and pupils should be handled very carefully. Staff should only email such information using **secure** email accounts provided by the school.
- Personal data should only be transferred to memory sticks that are encrypted.
- Teachers should not store personal data and information about pupils on their school laptops, unless it is encrypted; such data should be stored on encrypted memory sticks or on the school's server.
- Staff passwords will be 'strong', kept confidential and changed regularly.

**The Computing lead is Rachel Gooch
DSL is Alexis King.**

This policy was reviewed in September 2025

Christ the King Social Media code of conduct

Using Social Media correctly

- **Never use a pupils' name in the tweet.**
- **The purpose of the Social Media account is to showcase what your class/the school is doing.**
- **The Social Media account is not for informing parents about school admin e.g. dates.**

Types of Photograph to be used ,

Action shots where the children are not posing would be preferred. They could be reading their work to the class or a whole table could be hard at work looking focused. Remember anything we Social Media posts is a representation of our school.