Online Safety Policy for 2026

Policy Leader	**Mrs C Jones**
Last Updated	**January 2026**
Approved by the Governors	**February 2026**
Date to Review	**Annually**

Online Safety Policy for 2026

Mission Statement

"Love one another as I have loved you" (John, 15)

We believe that Jesus Christ and his Gospel Call – to love God and all people – are at the heart of what we do.

He inspires us, as children of God, to uphold the dignity of each individual.

We strive to develop a community in Christ which fully supports all in achieving their potential – spiritually, academically and personally.

Context

The wide scale use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. At Christ the King Catholic High School we believe that an effective approach to online safety empowers us to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- **content**: being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views
- **contact**: being subjected to harmful online interaction with other users; for example, inappropriate commercial advertising, phishing and or scams as well as adults posing as children or young adults; and
- **conduct**: personal online behaviour that increases the likelihood of or causes harm; for example, making, sending and receiving explicit images, or online.

The requirement to ensure that children and young people can use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The school online safety policy will help to ensure safe and appropriate use and is an integral part of the school's robust safeguarding procedures and its duty under Keeping Children Safe in Education 2025.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- Risk of radicalisation through social media and the use of the internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Online bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files

- The potential for excessive use which may impact on the social and emotional well-being and development and learning of the young person

Many of these risks reflect situations in the off-line world and it is essential that this online policy is used in conjunction with other school policies (Behaviour, Anti-bullying, and Safeguarding & Child Protection policies).

As with all other risks, it is impossible to eliminate those concerns completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Online safety encompasses not only internet technologies but also electronic communications via mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.

This policy applies to all members of the school community (including staff, students, governors, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006* empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying, or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports as part of Headteacher's termly report.

The nominated Safeguarding Governor (Mrs C Monaghan) has taken on the role of Online Safety Governor

The role of the Online Safety Governor will include:

- Liaising with Online Safety Designated person
- Reporting to relevant Governors' committee / meeting

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community

- The leadership team members are responsible for ensuring that the Online Safety Person and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant

- A member of the Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles (network filtering supervision, appropriate use of IT consent for students and spot checks for example)

- The Headteacher and Designated Safeguarding Lead follow relevant procedures in the event of a serious online safety allegation being made against a member of staff.

Online Safety Designated person:

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents

- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place, including recording of incidents on CPOMS.

- Organises training and advice for staff

- Liaises with the Local Authority

- Liaises with school ICT technical staff

- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments

- Liaises with Online Safety Governor to discuss current issues

- Attends relevant meeting / committee of Governors

- Reports regularly to Senior Leadership Team

IT/Technical staff:

The Network Manager is responsible for ensuring:

- The school's ICT infrastructure is secure and is not open to misuse or malicious attack

- The school meets the online safety technical requirements outlined in the school's Acceptable Usage Policy and any relevant Local Authority Online Safety guidance

- Users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed

- The school's filtering procedure is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

- They keep up to date with e-safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

- The use of the network / Virtual Learning Environments (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction

- That monitoring software / systems are implemented and updated as agreed in school procedures.

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school online safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the Online Safety Designated person / ICT Co-ordinator/Network Manager for investigation / action / sanction via Technical Services / record on CPOMS if appropriate
- Digital communications with students (email / Virtual Learning Environment (VLE)) should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other school activities
- Students understand and follow the school online safety and acceptable use policy
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Staff ensure that online safety education and support are adapted to meet the needs of SEND, EAL and other vulnerable groups, enabling them to engage safely and confidently with digital technologies
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated person for child protection

Should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Online bullying
- Online materials related to extremism and radicalisation

Students:

- Are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school systems
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking / use of images and online bullying
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local online safety campaigns / literature. Parents and carers will be responsible for: • Endorsing (by signature) the Student Acceptable Use Policy

Policy Statement – EDUCATION

Education – How students are taught to keep themselves safe

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks including exploitation and extremism and build their resilience to these risks.

Online safety education will be provided in the following ways:

- A planned online safety programme should be provided as part of ICT / PSHE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key online safety messages should be reinforced as part of a planned programme of assemblies

Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

- Students should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all rooms
- Students should adhere to rules regarding phone use in school: to be out of sight before students enter the school site and only to be accessed again after 3pm outside of the school building

Education – Parents/Carers

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, Christ the King Catholic High School website, VLE and social media updates
- Parents' evenings

Education & Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Online safety training will be made available to staff
- Staff are familiar with the guidance related to Online Safety in Keeping children safe in education 2025
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies
- Where applicable the Headteacher will receive regular updates from the IT Technical staff, Designated Safeguarding Lead and Family Support Worker through attendance at LA / other information / training sessions and by reviewing guidance documents released by the local authority and others
- This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days

Through liaison with the Senior Assistant Headteacher relevant CPD will take place as required

Education &Training – Governors

- Attendance at training provided by the Diocese / Local Authority / National Governors Association or other relevant organisation.

Policy Statement TECHNICAL/SOFTWARE

Infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Technicians
- All users will be provided with a username and password by (Technicians) who will keep an up-to-date record of users and their usernames
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- In the event of the Technicians needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher
- Requests from staff for sites to be removed from the filtered list will be considered by the Technicians
- School ICT technical staff monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy

An appropriate system is in place for users to report any actual / potential online safety incident (link on the school website / CEOP / Report Harmful content / Report-remove)

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, handheld devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, visitors) onto the school system
- An agreed policy is in place that restricts staff from installing programmes on school workstations/portable devices
- The school infrastructure and individual workstations are protected by up-to-date virus software

Curriculum

Online safety education will be embedded explicitly across the curriculum, with measurable learning outcomes at each key stage. Staff will receive ongoing professional development to integrate online safety into all subject areas, supporting the school’s priority to develop

literacy, critical thinking, and independent learning skills aligned with the OFSTED framework

- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that IT support can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students will receive age-appropriate online safety information within the school curriculum which focusses on how to stay safe, protect themselves from harm and how to take responsibility for their own online safety and that of others

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images

- Parents or carers will have the option to opt in for any photographs of students which are to be used for educational or marketing purposes

Procedures for use of the internet and email

- All users must sign an 'Acceptable Use Agreement' before access to the Internet and email is permitted in the establishment
- Users must access the Internet and e-mail using their **own** IT account and **NOT** those of another individual. If users feel their passwords are compromised, they must report it to Staff/IT Services
- The Internet and e-mail must be used in a reasonable manner adhering to the professional judgment of the supervising member of school staff
- Students must be always supervised when using the Internet and e-mail in school
- Procedures for safe Internet use and sanctions are applicable if rules are broken
- Internet and e-mail filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam,' junk or unwanted correspondence. This is to be reviewed and updated regularly
- Internet and e-mail use will be monitored regularly in accordance with the Data Protection Act 2018
- Users must be careful when they disclose any information of a personal nature in an email or on the Internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified
- All e-mails sent should be courteous and the formality and tone of the language used appropriate to the reader. Sanctions, appropriate to the case, will be imposed on any users who break this code
- Bullying, harassment or abuse of any kind via e-mail will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code
- If users are bullied, or offensive e-mails are received, this must be reported immediately to a trusted adult or member of staff within the service / establishment. emails received should not be deleted, but kept for investigation purposes
- Copyright must not be broken

Use of emerging technologies - The following platforms are used at Christ the King (subject to change)

- Co-Pilot
- CHAT GTP
- SLT AI
- Facebook

Before new digital technologies or platforms are introduced for educational use, a risk assessment must be completed and approved by the Senior Leadership Team, Online

Safety Designated Person and IT/Technical staff to ensure safety and compliance. Please see separate document AI Statement January 2026

Communications

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access)
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and students or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

Procedures for use of a shared network

Users must access the network using their own accounts. These must not be disclosed or shared

- Users must respect confidentiality and attempts should not be made to access another individual's account or files on the network without permission
- Software should only be installed by the IT Services
- Users must ensure they have adequate virus protection on any machine on which they use removable media before it is used in school
- Machines must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.' (Ctrl+Alt+Del followed by 'lock computer')
- Machines must be 'logged off' correctly after use

File transfer

Files may be taken home or brought into school by students by using Microsoft One Drive. Remember, the school uses special filtering software, which prevents you from accessing most unsuitable sites and it also records every attempt you make to hit a site, whether successful or not, when and where you did it and who you are. So, remember every action you take under your account is recorded, and may be accompanied by screenshots and/or recordings of your session.

Procedures to ensure safety of Christ the King Catholic High School website

- All content and images must be approved before being uploaded onto the website prior to it being published
- The website is checked every term to ensure that no material has been inadvertently posted, which might put students or staff at risk
- Copyright and intellectual property rights are respected
- Permission is obtained via the data collection sheet from parents or carers before any images of students can be uploaded onto the website
- When photographs are used on the website, names of individuals will not be used as file names

Procedures for using mobile phones, digital and other devices

- The school is **NOT** responsible for students' personal mobile technology damaged, lost or stolen. Items are brought to school at your own risk.

- Students **MUST** switch off and securely store personal mobile devices during school hours unless explicitly permitted by teaching staff for educational purposes. Unauthorised use will result in confiscation, recorded sanctions, and parent/carer notification. Staff must not access, copy, or distribute images or content from students' personal devices. Clear guidance on consequences for misuse will be communicated regularly

- The use of games consoles will not be permitted in school at any time. Students may use school issued e- readers (e.g. iPads/Kindles) as part of literacy developments and other e-reading

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse i.e.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Online terrorist and extremist material
- Other criminal conduct, activity or materials

If any apparent or actual misuse appears to involve illegal activity the school will act accordingly and liaise with the Police and Local authority where appropriate.

If a student breaks any of the rules, consequences could be:

- A temporary ban on the use of all computer facilities at school until the situation is resolved.
- Appropriate punishment within the departmental and/or school pastoral systems

- A letter informing parents / carers what has occurred
- Contact with the Police, depending on the nature of the image and the age of the people involved.
- Any other action decided by the Headteacher and Governors of the school

The school recognises that online safety extends beyond the school site. Students are encouraged and supported to adopt safe and responsible online behaviours at home and in the community. Where incidents linked to the school occur off-site, appropriate action will be taken in line with the school's behaviour and safeguarding policies

Data Protection

The school complies fully with the GDPR and Data Protection Act 2018, ensuring that personal data is processed lawfully, transparently, and securely. Staff and students are trained on data privacy principles, and the importance of safeguarding personal information online. Please see the Mater Ecclesiae Catholic Multi Academy Trust Data Protection Policy.

Monitoring and Evaluation of Online Safety

Regular monitoring and evaluation of the online safety policy's effectiveness will be conducted through data analysis of incidents, staff and student feedback, and audit of training uptake. Findings will be reported to Governors and inform continuous improvement, ensuring alignment with school priorities and statutory requirements