# CHRIST THE KING CATHOLIC HIGH SCHOOL AND SIXTH FORM CENTRE

## Online Safety Policy

# Background/Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students/ pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to 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. A school Online Safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils/students themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil/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 – Child Sexual Exploitation
- ✓ the sharing/distribution of personal images without an individual's consent or knowledge
- ✓ inappropriate communication/contact with others, including strangers
- ✓ cyber-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 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 Safety policy is used in conjunction with other school policies (eg Behaviour, Anti-Bullying and Safeguarding policies).

The school must demonstrate that it has provided the necessary safeguards to help ensure they have done everything that could reasonably be expected of them to manage and reduce these risks. The Online Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

## Scope of the Policy

This policy applies to all members of the school community (including staff, students/ pupils, 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 pupils/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 cyber-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 anti-bullying 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/Governors' Ethos, Behaviour and Safety Sub-Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor .The role of the Online Safety Governor will include:

➢ regular meetings with the Online Safety Coordinator
➢ regular monitoring of Online Safety incident logs
➢ regular monitoring of filtering/change control logs
➢ reporting to relevant Governors committee/meeting

## Online Safety Policy

### Headteacher and Senior Leaders:

➢ The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Coordinator

➢ The Headteacher/Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues as relevant

➢ The Headteacher/Senior Leaders will ensure 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

➢ The Senior Leadership Team will receive regular monitoring reports from the Online Safety Coordinator

➢ The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff

### Online Safety Coordinator:

➢ leads the Online Safety committee

➢ 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

➢ provides 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

➢ meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs

➢ attends relevant sub-committee of Governors

➢ reports regularly to Senior Leadership Team

## Online Safety Policy

### Systems Manager/Technical staff are responsible for ensuring:

➢ that the school's ICT infrastructure is secure and is not open to misuse or malicious attack

➢ that the school meets the online safety technical requirements outlined in the Acceptable Use Policy and any relevant Local Authority Online Safety policy and guidance

➢ that 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 policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.

➢ that he / she keeps up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant

➢ that the use of the network/Virtual Learning Environment (VLE)/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Online Safety Co-ordinator/Headteacher/Senior Leader/Head of ICT / ICT Coordinator/ class teacher/Head of Year (as in the section above) for investigation/action/sanction

➢ that monitoring software/systems are implemented and updated as agreed in school policies

### 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 Coordinator/ Systems Manager  for investigation/action/sanction

➢ digital communications with pupils/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

➢ pupils/students understand and follow the school Online Safety and Acceptable Use policies

➢ pupils/students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

➢ 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 pupils 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

## Online Safety Policy

### Designated Safeguarding Leads:

➢ should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:
- ➢ sharing of personal data
- ➢ access to illegal/inappropriate materials
- ➢ inappropriate online contact with adults/strangers
- ➢ potential or actual incidents of grooming
- ➢ cyber-bullying

### Online Safety Committee

Members of the Online Safety committee will assist the Online Safety Coordinator (or other relevant person, as above) with:
➢ the production/review/monitoring of the school Online Safety Policy/documents.

### Pupils/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 procedures on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school procedures on the taking/use of images and on cyber-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
➢ accessing the school website/VLE in accordance with the relevant school Acceptable Use Policy

# Policy Statements

## Education – Pupils/Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students pupils to take a responsible approach. The education of pupils/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 and build their resilience.

Online safety education will be provided in the following ways:

➢ A planned online safety programme should be provided as part of ICT/Guidance/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 and tutorial / pastoral activities
➢ Pupils/students should be taught in all lessons to be critically aware of the materials/ content they access online and be guided to validate the accuracy of information
➢ Pupils/students should be helped to understand the need for the student/pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
➢ Pupils/students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
➢ Staff should act as good role models in their use of ICT, the internet and mobile devices

## Education – Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide" (Byron Report).

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

➢ Letters, newsletters, web site
➢ Parents evenings

## Online Safety Policy

### 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:

➤ Updated online training sessions will be held as deemed appropriate as part of our general safeguarding training programme

➤ All new staff should receive information on online safety as part of their induction programme, ensuring that they fully understand the school Online Safety and Acceptable Use policies

➤ This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings/INSET days

➤ The Online Safety Coordinator will provide advice/guidance/training as required to individuals

### Training – Governors

Governors should take part in Online Safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in ICT/ Online safety/health and safety/safeguarding. This may be offered in a number of ways:

➤ Attendance at training provided by the Local Authority or other relevant organisation

➤ Participation in school training / information sessions for staff or parents

### Technical – 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

➤ There will be regular reviews and audits of the safety and security of school ICT systems 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 Systems Manager and will be reviewed, at least annually, by the Online Safety Committee

➤ All users will be provided with a username and password by ICT Support staff 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 The school maintains and supports the managed filtering service provided by Sefton LA

# CHRIST THE KING CATHOLIC HIGH SCHOOL AND SIXTH FORM CENTRE

## Online Safety Policy

- The school has provided enhanced user-level filtering through the use of the Censornet filtering system
- In the event of the Systems Manager (or other person) 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 (or Online Safety Coordinator)
- Any filtering issues should be reported immediately to ICT Support staff
- Requests from staff for sites to be removed from the filtered list will be considered by the Systems Manager and the Online Safety Coordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Committee
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy
- Remote management tools are used by staff to control workstations and view users activity
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held 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" (eg trainee teachers, visitors) onto the school system
- An agreed policy is in place regarding the downloading of executable files by users
- An agreed policy is in place regarding the extent of personal use that users (staff/ pupils/students/community users) and their family members are allowed on laptops and other portable devices that may be used out of school
- An agreed policy is in place that allows staff to/forbids staff from installing programmes on school workstations / portable devices
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations/portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured
- The school employs a keyword monitoring system that logs words typed on school computers/Access 24.  Email alerts are sent to the Designated Safeguarding Lead/Online Safety Coordinator and appropriate action takes place which may include: speaking to the pupils, informing parents/carers, recording on behaviour monitoring system, referral to external agencies.  A monthly report is provided by the System Manager for discussion with the Online Safety Coordinator

## Curriculum

**Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.**

➢ In lessons where internet use is pre-planned, it is best practice that pupils/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 pupils/students are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

➢ Pupils/students should be taught in all lessons to be critically aware of the materials/ content they access online and be guided to validate the accuracy of information

➢ Pupils/students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

## Use of Digital and Video Images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils/students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils/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. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. 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 pupils/students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg 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 pupils/students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute

➢ Pupils/students must not take, use, share, publish or distribute images of others, without their permission

➢ Photographs published on the website, or elsewhere that include pupils/students will be selected carefully and will comply with good practice guidance on the use of such images

- Pupils'/students' full names will not be used anywhere on a website or blog, particularly, in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils/students are published on the school website
- Pupils'/student's work can only be published with the permission of the pupil/student and parents or carers.

## Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- kept no longer than is necessary
- processed in accordance with the data subject's rights
- secure
- only transferred to others with adequate protection

**Staff must ensure that they:**
- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- transfer data using encryption and secure password protected devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

# CHRIST THE KING CATHOLIC HIGH SCHOOL AND SIXTH FORM CENTRE

# Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

| Communication Technologies | Staff & Other Adults | | | | Pupils/students | | | |
|---|---|---|---|---|---|---|---|---|
| | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| Mobile phones may be brought to school | ✓ | | | | ✓ | | | |
| Use of mobile phones in lessons | | | | ✓ | | | | ✓ |
| Use of mobile phones in social time | ✓ | | | | ✓ | | | |
| Taking photos on mobile phones or other camera devices | | | | ✓ | | | | ✓ |
| Use of hand-held devices, eg PDAs, PSPs | | | | ✓ | | | | ✓ |
| Use of personal email addresses in school or on school network | | | | ✓ | | | | ✓ |
| Use of school email for personal emails | | | | ✓ | | | | ✓ |
| Use of chat rooms/facilities | | | | ✓ | | | | ✓ |
| Use of instant messaging | | | | ✓ | | | | ✓ |
| Use of social networking sites | | | | ✓ | | | | ✓ |
| Use of blogs | | ✓ | | | | | ✓ | |

# CHRIST THE KING CATHOLIC HIGH SCHOOL AND SIXTH FORM CENTRE

## Online Safety Policy

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 pupils/students should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access)

➢ Users need to be aware that email communications may be monitored

➢ Users must immediately report, to the nominated person – in accordance with the school policy, 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 pupils/students or parents/carers (email, chat, VLE etc) must be professional in tone and content

➢ Pupils/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

# Unsuitable/Inappropriate Activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

| | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|
| **Child sexual abuse images** | | | | | ✔ |
| **Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation** | | | | | ✔ |
| **Adult material that potentially breaches the Obscene Publications Act in the UK** | | | | | ✔ |
| **Criminally racist material in the UK** | | | | | ✔ |
| **Pornography** | | | | ✔ | |
| **Promotion of any kind of discrimination** | | | | ✔ | |
| **Promotion of racial or religious hatred** | | | | | ✔ |
| **Threatening behaviour, including promotion of physical violence or mental harm** | | | | | ✔ |
| **Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute** | | | | ✔ | |
| **Using school systems to run a private business** | | | | ✔ | |

| Activity | | | | | |
|---|---|---|---|---|---|
| **Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school** | | | | ✓ | |
| **Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions** | | | | | ✓ |
| **Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)** | | | | | ✓ |
| **Creating or propagating computer viruses or other harmful files** | | | | | ✓ |
| **Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet** | | | | ✓ | |
| **Online gaming (educational)** | | ✓ | | | |
| **Online gaming (non-educational)** | | | | ✓ | |
| **Online gambling** | | | | ✓ | |
| **Online shopping/commerce** | | | ✓ | | |
| **File sharing** | | | ✓ | | |
| **Use of social networking sites** | | | | ✓ | |
| **Use of video broadcasting eg Youtube** | | ✓ | | | |