St Cuthbert's
ROMAN CATHOLIC ACADEMY TRUST

Online Safety Policy

Date policy produced:	September 2020
Last Reviewed	September 2023
Next review:	September 2024, or sooner if necessary

Policy Statement

Aims

Our Trust aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and directors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones' , 'smart watches' etc.)
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, homophobia, biphobia, transphobia, 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, D-Dos attacks and/or financial scams

For clarity, our Online Safety Policy uses the following terms unless otherwise stated:

Users	refers to all staff, pupils, Directors, volunteers and any other person working in or on behalf of the Trust, including contractors.
Parents	any adult with a legal responsibility for the child/young person outside the Trust schools e.g. parent, guardian, carer.

Online safety is an integral part of safeguarding and requires a whole school approach. This policy is written in line with Keeping Children Safe in Education (2023) and Teaching Online Safety in Schools (2019). It also takes into account the DfE

guidance on protecting children from radicalisation and the National Curriculum computing programmes of study.

Safeguarding is a serious matter and at St Cuthbert's RC Academy Trust we use technology and the internet extensively across all areas of the curriculum. Online safeguarding, known as Online Safety, is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an Online Safety incident, whichever is sooner.

The primary purpose of this policy is two-fold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk-free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce foreseeable harm to the pupil or liability to the school.

This policy is available for anybody to read on the St Mary's College website. As part of the induction process, all new staff will receive information and guidance on the Online Safety policy, the schools acceptable use policies, plus the reporting procedures.

A copy of the Pupil Acceptable Use/ Devices agreements will be sent home electronically, annually to pupils and families. Upon return of the completed agreement pupils will be permitted access to the school's technology, including the internet for the duration of their time with the school, unless this is withdrawn for any breach of the agreement.

Roles & Responsibilities

In our Trust, all members of our community have a duty to behave respectfully both online and offline. Technology will be used for teaching and learning and prepare our pupils for life after school.

The Board of Directors

The Directors have overall responsibility for ensuring that our schools have effective policies and procedures in place; as such they will:

- Hold the DSL / Head of School accountable for the implementation of the policy
- Review this policy at least annually and in response to any Online Safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure Online Safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- An appointed Director to have overall responsibility for the governance of Online Safety across the Trust and will:
  - Keep up to date with emerging risks and threats through technology use.
  - Receive regular updates from Head of School and DSL in regard to training, identified risks and any incidents.
  - Ensure that pupils are taught about how to keep themselves safe online.

Heads of School

The Head of School has overall responsibility for Online Safety and ensuring the policy is implemented consistently within each school. The day-to-day management of this will be delegated to a member of staff (Designated Safeguarding Lead), as indicated below.

The Head of School will ensure that:

- There is a culture of safeguarding where Online Safety is fully integrated into whole-school safeguarding.
- Online Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e., pupils, all staff, senior leadership team, other stakeholders and parents.
- The Designated Safeguarding Lead has had appropriate training in order to support online safety.
- All Online Safety incidents are dealt with promptly and appropriately, in accordance with related policies and procedures.
- Suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including the risk of pupils being radicalised.
- Data management and information security is compliant with GDPR

Designated Safeguarding Lead/Online Safety Lead

The Designated Safeguarding Lead (DSL) is identified in the school's Safeguarding Policy, they will take the lead responsibility for safeguarding and child protection, including Online Safety, as per Keeping Children Safe in Education. However, the DSL may delegate certain Online Safety functions to other members of the Trust eg ICT Support Services.

The DSL will:

- Support the Head of School in ensuring the policy is implemented consistently within each school.
- Keep up to date with the latest risks to children whilst using technology, familiarising themselves with the latest research and available resources for school and home use.
- Ensure there is an effective approach to Online Safety which empowers the school to protect and educate in the use of technology and establish mechanisms to identify, intervene, and escalate any incident, where appropriate.
- Review this policy regularly and bring any matters to the attention of the Head of School.
- Advise the Head of School and Stakeholders on all Online Safety matters.
- Engage with parents and the school community on Online Safety matters at school and/or at home.
- Liaise with ICT technical support, or other agencies as required.
- Retain responsibility for the Online Safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical Online Safety measures in the school (e.g. Securly internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT technical support.
- Make themselves aware of any reporting function with technical Online Safety measures, i.e. internet filtering reporting function; liaise with the Head of School

and responsible governor to decide on what reports may be appropriate for viewing.

This list is not intended to be exhaustive.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that the IT technical infrastructure is secure; this will include as a minimum:

- We hold the Cyber Essentials standard
- Comply with the CIS benchmark standards
- RPA cyber compliance

This list is not intended to be exhaustive.

All Staff

Staff including contractors and agency staff are to ensure that:

- All details within this policy are understood, maintained and applied consistently. If anything is not understood it should be brought to the attention of the DSL or Head of School.
- Any Online Safety incident (including cyber bullying and sexual harassment online) is reported to the DSL (and an Online Safety incident report is made) or in their absence, to the Head of School. If you are unsure, the matter is to be raised with the DSL or the Head of School to make a decision.
- Agreeing and adhering to the terms of acceptable use of the schools ICT systems and internet and ensuring pupils follow these.
- Part 1 and Annex C of Keeping Children Safe in Education is read and understood.
- The Securly system is implemented by staff in the classroom as expected.
- All online material is checked fully before using either within the classroom or remotely
- The reporting flowcharts contained within this Online Safety policy are fully understood.
- The DSL is informed if this policy does not reflect practice, or if concerns are not acted upon promptly.

This list is not intended to be exhaustive.

All pupils

The boundaries of use of ICT equipment and services in this school are given in the Pupil Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the Behaviour Policy.

Online Safety is embedded into our Digital Literacy curriculum; pupils will be given the appropriate advice and guidance by staff. Similarly, all pupils will be fully aware how they can report areas of concern whilst at school or outside of school. Our curriculum will give pupils an understanding of the benefits and opportunities, plus risk and dangers associated with the online world and know who to talk to if problems occur.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge, they need to ensure the safety of children outside the school environment. Through parents' evenings, communications home, school social media and the website, the school will keep parents up to date with new and emerging Online Safety risks and will involve parents in strategies to ensure that pupils are empowered. Parents are expected to notify a member of staff or the head of school of any concerns or queries regarding this policy. Online safety will also be covered during parents' evenings.

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will sign the Pupil Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Curriculum

It is important that pupils are sufficiently empowered with the knowledge to stay as risk-free, as possible, whilst using digital technology. Our pupils are taught about safeguarding, including online safety, through teaching and learning opportunities, as part of a broad and balanced curriculum. We use different aspects of the curriculum, such as PSHE, ICT, SMSC, and Relationships and Health Education to educate pupils on how to keep themselves safe, build their resilience, plus manage online risks.
Staff will ensure that there are positive messages about the safe use of technology and risks are discussed at an age-appropriate level. Our Trust actively participates in annual national events, such as Internet Safety week which aims to inspire a national conversation about using technology responsibly, respectfully, critically, and creatively.

All of our schools have to teach:

- Relationships and Health Education in primary schools
- Relationships and Sex and Health Education in secondary schools

Secondary schools:

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

All of our schools will teach

- 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.

Special Educational Needs & Disability (SEND)

The Trust recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and Looked After Children (LAC). Relevant members of staff from within each individual academy, e.g. the SENDCo and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

Filtering and monitoring

Leaders have ensured that the Trust has age and ability-appropriate filtering, monitoring and advanced AI online wellness proactive tools in place to limit pupils' exposure to online risks. The Trust is aware of the need to prevent "over blocking", as that may unreasonably restrict what pupils can be taught, with regards to online activities and safeguarding. Filtering and monitoring systems have been informed by a risk assessment, taking into account specific needs and circumstances and any changes to this approach will be risk assessed by staff with educational and technical experience and consent from the leadership team. Individual academy leaders will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate. As a Trust, we acknowledge that we cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is also essential. ICT technicians undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Secondary Schools ONLY

Mobile Technology - the college recognises that mobile technology does not go through our web filtering system. As such we educate the pupils via PSHE lessons and assemblies about the importance of staying safe online. With the Acceptable Use policy, we aim to minimise the risks to our pupils. Any use of mobile technologies to intimidate, threaten or cause harm to others will be taken seriously, and if appropriate, action taken, in accordance with the college's Behaviour Policy. Mobile phones are only allowed in school in the Sixth Form.

USE OF DIGITAL AND VIDEO IMAGES

Staff are allowed to take digital/video images to support educational aims on a school device and where consent has been granted, but must ensure that all images are transferred to a secure area on the school network/encrypted laptop immediately on return to school (if from an off-site visit) and before the camera is removed from site (if taken on-site). Staff are encouraged to use school equipment to take digital images and should not use own devices unless given prior permission by the head of school. Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individual or the school into disrepute. Any images collected shall only be shared, used, published or distributed in a way that is agreed by parents, e.g. staff will show compliance with the consent form signed by every parent in the school. Images published on the school website will be selected carefully and will comply

with good practice guidance, e.g. names shall not be published with images (unless specific parental consent is granted) and all pictures will be within GDPR regulations.

The Data Protection Act 2018 does not apply to images of children taken purely for personal use by their parents/carers at an organised event. However, we do ask parents/cares to refrain from posting images on public forums, such as social media, so it does not adversely affect the safeguarding of pupils and staff.

Social networking

Our Trust is supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents/carers and the wider school community. Any form of social media developed on behalf of a Trust school can only be developed in line with the Trust's strategy and with written permission from the Head of School/Marketing & Communications Manager. Any new social networking service will be risk assessed before use is permitted.

Before anything is uploaded, to the academy's social media site, the following **must** be applied:

- The account details including username and password log- in details should be shared with the Head of School and/or the Marketing & Communications manager
- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of pupil using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to or regularly "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license which allows for such use (i.e. creative commons).

Notice and take-down policy

Should it come to the Trust's attention that there is a resource or image which has been inadvertently uploaded, and the school does not have copyright or permission to use, it will be removed within one working day.

CCTV

Schools may use CCTV in areas of school property as a security measure. Cameras will only be used in appropriate areas. It will be used for the purpose of securing the safety and wellbeing of the pupils, staff and school together with its visitors.

Incidents

It is vital that all staff recognise that Online Safety is a part of safeguarding.

The Trust commits to take all reasonable precautions to ensure online safety but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into

school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes. Any suspected online risk or infringement should be reported to the designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.
Any concern/allegation about staff misuse is always referred directly to the Head of School, unless the concern is about the Head of School in which case the compliant is referred to the Chair of the Trust and the LADO (Local Authority's Designated Officer).
The school will actively seek support from other agencies as needed (i.e. the local authority -Children's Social Care, National Crime Agency, CEOP, Police, IWF). We will inform parents/carers of Online Safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for child sexual imagery, sexting, up skirting etc).

Behaviour

Online communication can take many forms, whether it is by email, text, webcam or instant chat. It is essential that all staff and learners are aware of the Trust's policies that refer to acceptable behaviours when communicating online.

- the Trust will ensure that all users of technologies sign and adhere to the standard of behaviours set out in the Acceptable Use Policy
- the Trust will not tolerate any abuse of its ICT network, infrastructure or cloud-based systems, whether offline or online. All communications by staff and pupils should be courteous and respectful at all times.
- any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously.

Where conduct is found to be unacceptable, the Trust will deal with the matter internally. Where conduct is considered to be illegal, the Trust will report the matter to the police and other relevant external organisations as required/instructed.

Online sexual harassment

Sexual harassment is likely to: violate a child's dignity, make them feel intimated, degraded or humiliated and/or create a hostile, offensive or sexualised environment. Online sexual harassment, which might include non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as 'sexting'; inappropriate sexual comments on social media; exploitation; coercion and threats). Any reports of online sexual harassment will be taken seriously, and the police and Children's Social Care may be notified**. Staff should never view any devices with alleged child sexual images and should always record accurately what has been reported.** Our Trust follows and adheres to the national guidance - UKCCIS: Sexting in schools and colleges: Responding to incidents and safeguarding young people.

Screening, Searching and Confiscation

The Education Act 2011, allows staff to lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

- cause harm,
- disrupt teaching,
- break school rules,
- commit an offence,
- cause personal injury, or
- damage property.

Radicalisation Procedures and Monitoring

We will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school and that suitable filtering is in place which takes into account the needs of pupils.

When concerns are noted by staff that a pupil may be at risk of radicalisation online then the Designated Safeguarding Lead will be informed immediately, the incident will be logged, and action will be taken in line with the Trust's Child Protection/Safeguarding Policy.

A risk assessment (see appendices) considers the risks students face online and will take measures to mitigate these. Regular review is essential as risks and harm evolve rapidly.

Remote Learning

In the event of a full or partial closure, the Trust is committed to ensuring pupils continue with their learning. Wherever possible, academies within the Trust, will continue to deliver live lessons using Trust approved systems (e.g. Microsoft Teams, Google Classroom).

Staff who interact remotely with students will continue to look out for signs that a child may be at risk. Any such concerns will be dealt with as per the Trust's Child Protection policy and procedures, and where appropriate referrals will be made to Children's Social Care, and/or the Police.

St Cuthbert's RC Academy Trust
Acceptable Use Policy – Staff, Directors, Volunteers & Visitors

Note: All Internet and email activity is subject to monitoring

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.

Print full name:

Signature:

Date:

Circle one: staff member / director / volunteer / visitor

St Cuthbert's RC Academy Trust
SM6 BYOD agreement

St Mary's College recognises that digital technologies have become integral to children's and young people's lives. These technologies can stimulate discussion, creativity, and context awareness to promote effective learning. Therefore, young people should have access to these digital technologies. Part of the College's vision is to ensure that all our young people have the digital skills to learn effectively, work productively and live safely in modern-day society.
Sixth-form students wishing to use their devices on the school site must adhere to the following:

- Students will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *learners* to agree to be responsible users.

BYOD Agreement

I understand that I must responsibly use the school system to ensure that there is no risk to my safety and the security of the systems and other users.

- I am fully responsible for my device(s). However, I understand that The School is not responsible for the device(s) in any way.
- I am not permitted to leave my device(s) on school premises outside of school hours.
- When not in use for educational purposes, my device(s) must be left 'on silent' to prevent any disruption to learning.
- I must immediately comply with any teacher's requests to put away and shut down or close the screen on my device(s).
- I understand that I am not permitted to transmit or upload photographic images/videos of any person on The School site.
- I am responsible for charging my device(s) before bringing it/them to school so it/they can run on their batteries whilst at school. Charging may only sometimes be available, and it will always be at teachers' discretion.
- I understand that The School will not accept any responsibility for damage to my device under any circumstances, including damage caused by connecting to the school network and any infection by malware (i.e. viruses, worms, ransomware, spyware, adware, scareware and other malicious programs).
- To ensure appropriate internet filters are in place, I understand that I can only use The School BYOD Wi-Fi in the school network and will not attempt to bypass the network restrictions by using a 3G/4G/5G network.
- I understand that I must take all reasonable steps to avoid bringing devices onto The School premises that might infect the network with a virus, worm or any

program designed to damage, alter, destroy, or provide access to unauthorised data or information. Failure to do so violates the responsible student's acceptable use policy and will result in disciplinary action under the school's behaviour policy.

- I accept that The School has the right to examine any device suspected of containing material that contravenes the school rules or is the source of an attack or virus infection.
- I understand that if I share my device(s) with other students, the device remains my responsibility. Or I can choose not to share my device.
- I agree that my device(s) cannot be used during tests or assessments unless explicitly directed by a teacher.
- Voice, text messages, pictures or videos must never be sent or received in lessons, social time, assemblies, interviews, tests and examinations. Furthermore, the exam boards stipulate that using phones in examinations will lead to disqualification.

Student BYOD Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. You must sign and return this agreement, the school can grant access to school systems.

I have read and understand the above and agree to follow these guidelines.

Name of Learner: _____
Group/Class: _____
Signed: _____
Date: _____

Acceptable Use Policy – Pupils

Our Charter of Good Online Behaviour

(Note: All Internet and email activity is subject to monitoring)

- **I Promise** – to only use the school ICT for schoolwork that the teacher has asked me to do.
- **I Promise** – not to look for or show other people things that may be upsetting.
- **I Promise** – to show respect for the work that other people have done.
  - **I will not** – use other people's work or pictures without permission to do so.
  - **I will not** – damage the ICT equipment, if I accidentally damage something I will tell my teacher.
  - **I will not** – share my password with anybody. If I forget my password I will let my teacher know.
  - **I will not** – use other people's usernames or passwords.
  - **I will not** – share personal information online with anyone.
  - **I will not** – download anything from the internet unless my teacher has asked me to.
  - ✓ **I will** – let my teacher know if anybody asks me for personal information.
  - ✓ **I will** – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.
  - ✓ **I will** – be respectful to everybody online; I will treat everybody the way that I want to be treated.

I understand – that some people on the internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Parent):

Signed (Pupil):

Date:

Response to Risk Flowchart

Response to and Reporting of an Online Safety Incident of Concern