St Cuthbert's
ROMAN CATHOLIC ACADEMY TRUST

E-Safety Policy

ST MARY'S COLLEGE

Date policy produced: September 2020
Next review: September 2022, or sooner if necessary

Other related school policies that support this E-Safety Policy include:
Whistle Blowing, Anti Bullying, Safeguarding Children/Child Protection, Behaviour, Health & Safety, Data Protection & RSHE

Policy Statement

For clarity, the E-Safety Policy uses the following terms unless otherwise stated:

Users refers to all staff, pupils, governors, volunteers and any other person working in or on behalf of the school, including contractors.

Parents any adult with a legal responsibility for the child/young person outside the school 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 and Teaching Online Safety in Schools' 2019.

Safeguarding is a serious matter and at St Mary's College we use technology and the internet extensively across all areas of the curriculum. Online safeguarding, known as e-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 e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- 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 any foreseeability of 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 e-safety policy, the schools acceptable use policies, plus the reporting procedures.

A copy of this policy and the Pupil Acceptable Use Policy will be sent home with pupils at the beginning of each academic year with a permission slip. Upon return of the signed permission slip, showing acceptance of the terms and conditions, pupils will be permitted access to the school's technology, including the internet.

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 Trustees

The Trustees are accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- An appointed Trustee to have overall responsibility for the governance of e-safety across the Trust and will:

- Keep up to date with emerging risks and threats through technology use.
- Receive regular updates from the Headteacher in regard to training, identified risks and any incidents.
- Ensure that pupils are taught about how to keep themselves safe online.

Headteacher

The Headteacher has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff (Designated Safeguarding Lead), as indicated below.

The Headteacher will ensure that:

- There is a culture of safeguarding where e-Safety is fully integrated into whole-school safeguarding.
- E-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 E-Safety Officer has had appropriate training in order to undertake the day to day duties.
- All e-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 risk of pupils being radicalised.
- Data management and information security is compliant with GDPR

Designated Safeguarding Lead/E-Safety Lead

The Designated Safeguarding Lead (DSL) should take the lead responsibility for safeguarding and child protection, including e-Safety, as per Keeping Children Safe in Education. However, the DSL may delegate certain e-Safety functions to other members of the Trust eg ICT Support Services.

The DSL will:

- 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 e-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 Headteacher.
- Advise the Headteacher and Stakeholders on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Liaise with ICT technical support, or other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in the school (e.g. 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 e-safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

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

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Any e-safety technical solutions such as internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the DSL and/or Headteacher.
- Passwords are applied correctly to all users regardless of age and should be changed on a termly basis (as a minimum). Passwords for staff will be a minimum of 8 characters. *(Note: you should discuss age-appropriate passwords for pupils and apply this policy)*.
- The IT System Administrator password is to be changed on a monthly (30 day) basis.

All Staff
Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the DSL or Headteacher.
- Any e-safety incident is reported to the DSL (and an e-safety incident report is made) or in their absence, to the Headteacher. If you are unsure, the matter is to be raised with the DSL or the Headteacher to make a decision.
- Part 1 and Annex C of Keeping Children Safe in Education is read and understood.
- All online material is checked fully before using either within the classroom or remotely
- The reporting flowcharts contained within this e-safety policy are fully understood.
- The DSL is informed if this policy does not reflect practice, or if concerns are not acted upon promptly.

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.
E-Safety is embedded into our 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.

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, school newsletters and the website, the school will keep parents up to

date with new and emerging e-safety risks and will involve parents in strategies to ensure that pupils are empowered.

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 various 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 with effect from September 2020, 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.

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 and monitoring in place, to limit pupil's 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.

Internet filtering - we use software that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The DSL and ICT Technical Support Staff are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email filtering – we use software that prevents any infected email to be sent from the school or to be received by the school. Infected is defined as an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data or spam email such as a phishing message.

Encryption – all school devices that hold personal data (as defined by the Data Protection Act 2018) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB key drives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the Trust's Data Protection Officer to ascertain whether a report needs to be made to the Information Commissioner's Office. *(Note: Encryption does <u>not</u> mean password protected)*.

Passwords – all staff and pupils will be unable to access any device without a unique username and password. Staff and pupil passwords will change if there has been a compromise, whichever is sooner. The DSL and ICT Technical Support Staff will be responsible for ensuring that passwords are changed.

Anti-Virus – all capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. ICT Technical Support Staff will be responsible for ensuring this task is carried out and will report to the Headteacher if there are any concerns. All USB peripherals, such as key drives, are to be scanned for viruses before use.

Email – all staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Similarly, use of personal email addresses for work purposes is not permitted.

Mobile Technology - the college recognises that 3G and 4G 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 User policy, we aim to minimise the risks to our pupils. Any use of mobile technologies (e.g.3G, 4G, 5G or mobile internet services) 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.

USE OF DIGITAL AND VIDEO IMAGES

Staff are allowed to take digital/video images to support educational aims, but must ensure that these 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 teacher. 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 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 fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents/carers and the wider school community. Should staff wish to use any form of social media, permission must first be sought from Senior Leader who will advise the Headteacher for a decision to be made. 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:

- 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 "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 academy'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

The school may use CCTV in some areas of school property as a security measure. Cameras will only be used in appropriate areas and there is clear signage indicating where it is in operation. It will be used for the purpose of securing the safety and wellbeing of the pupils, staff and school together with its visitors. The Trust adheres to the Data Protection Act 2018, and guidance issued by the Information Commissioners Office (ICO).

Incidents

It is vital that all staff recognise that e-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 online safety lead / 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 Headteacher, unless the concern is about the Headteacher 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 e-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 academy policies that refer to acceptable behaviours when communicating online.

- the academy will ensure that all users of technologies sign and adhere to the standard of behaviours set out in the Acceptable Use Policy
- the academy 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 academy will deal with the matter internally. Where conduct is considered to be illegal, the academy 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 academy 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, and action will be taken in line with the Trust's Child Protection/Safeguarding Policy.

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 (eg Microsoft Teams). Staff who interact remotely with student 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.

Further advice and guidance is available via the Trust's COVID 19 addendum Child Protection policy and Contingency Plan and Remote Education.

St Cuthbert's RC Academy Trust
Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the E-Safety Policy. Once you have read and understood both you must sign this policy sheet.

Internet access - you must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the E-Safety Officer and an incident sheet completed.

Social networking - is not allowed on school premises and social network sites are blocked via the school internet. When making use of social networking off premises staff need to ensure they do not publish their association with the school (e.g. in their status), should never undermine the school, its staff, parents or children nor discuss any school matter. Staff should not become "friends" with parents or pupils on personal social networks.

Staff must set and maintain my profile settings on social networking sites to maximum privacy and give access to known friends only. Staff must not access social networking sites for personal use during school hours or using school equipment. If staff experience any derogatory or slanderous comments relating to the school, colleagues or own professional status, they will take screenshots for evidence and escalate to the E-Safety Officer.

Use of email - Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff, pupil or IT support.

Data protection - if it is necessary for you to take work home or off site, you should ensure that your device (laptop, USB, pen drive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal use of school ICT - any staff who have been issued with school laptops/iPads/tablets as part of their role in school (namely teachers, TAs and the Business Manager) have permission to use the devices at home and this may include personal use. However, each member of staff has a responsibility to ensure this device is password protected and appropriately used both inside and outside school.

Mobile phones and cameras - Staff must not use mobile phones in rooms where children are present, including those where children are cared for. It is appropriate to take photographs of children to capture a curriculum activity or a celebration of school life using school equipment providing we have permission to do so from the parents. Staff must not, however, use their personal mobile phone, camera (still or moving images) or other devices to take, edit or store images of children from this school. **(Also referenced in Safeguarding Children and Child Protection Policy 2020).**

Images and videos - you should not upload onto any internet site, service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of personal ICT - use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by ICT Technical Support Staff and the E-Safety Officer.

Viruses and other malware - any virus outbreaks are to be reported to the ICT Technical Support Staff as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

E-Safety - like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with students.

A reminder to staff - the internet provides students with access to a wide-range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages. The filtering system used by the Trust blocks inappropriate content, including extremist content. Where staff, pupils or visitors find unblocked extremist content they must report it to a senior member of staff.

NAME :

SIGNATURE : **DATE :**

St Cuthbert's RC Academy Trust

Acceptable Use Policy – Pupils (with parents)

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:

E-Safety Incident Log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Headteacher, E-Safety Officer)*
	When:	**When:**
Incident Description: (Describe what happened, involving which children and/or staff and what action was taken)		
Review Date:		
Result of Review:		
Signature (Headteacher)		**Date:**

Template Risk Log
(with a couple of examples)

No.	Activity	Risk	Likelihood	Impact	Score	Owner
1.	Internet browsing	Access to inappropriate/illegal content - staff	1	3	3	E-Safety Officer IT Support
1.	Internet browsing	Access to inappropriate/illegal content - students	2	3	6	
2.	Blogging	Inappropriate comments	2	1	2	
2.	Blogging	Using copyright material	2	2	4	
3.	Student laptops	Students taking laptops home – access to inappropriate/illegal content at home	3	3	9	

Likelihood: **How likely is it that the risk could happen (foreseeability).**
Impact: **What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc.)**

Likelihood and Impact are between 1 and 3, 1 being the lowest.
Multiply Likelihood and Impact to achieve score.

LEGEND/SCORE: 1 – 3 = Low Risk
4 – 6 = Medium Risk
7 – 9 = High Risk

Owner: **The person who will action the risk assessment and recommend the mitigation to Headteacher and Governing Body. Final decision rests with Headteacher and Governing Body**

Example Risk Assessment

Risk No.	Risk
3	In certain circumstances, pupils will be able to borrow school-owned laptops to study at home. Parents may not have internet filtering applied through ISP. Even if they do there is no way of checking the effectiveness of this filtering; pupils will potentially have unrestricted access to inappropriate/illegal websites/ services. As the laptops are owned by the school and the school requires the student to undertake this work at home, the school has a common law duty of care to ensure, as much as is reasonably possible, the safe and well-being of the child.
Likelihood 3	The inquisitive nature of children and young people is that they may actively seek out unsavoury online content or come across such content accidentally. Therefore, the likelihood is assessed as 3.
Impact 3	The impact to the school reputation would be high. Furthermore, the school may be held vicariously liable if a student accesses illegal material using school-owned equipment. From a safeguarding perspective, there is a potentially damaging aspect to the student.
Risk Assessment	HIGH (9)
Risk Owner/s	E-Safety Officer ICT Technical Support Staff
Mitigation	This risk should be actioned from both a technical and educational aspect: Technical: Laptop is to be locked down using St Mary's College software. This will mean that any Internet activity will be directed through the school Internet filter (using the home connection) rather than straight out to the Internet. The outcome is that the pupil will receive the same level of Internet filtering at home as he/she gets whilst in school. Education: The E-Safety Policy and Acceptable Use Policy will be updated to reflect the technical mitigation. Both the pupil and the parent will be spoken to directly about the appropriate use of the Internet. Parents will be made aware that the laptop is for the use of his/her child only and for school work only. The current school e-safety education programme has already covered the safe and appropriate use of technology, pupils are up to date and aware of the risks.

Approved / Not Approved (circle as appropriate) **Date:**

Signed (Headteacher) : **Signed (Governor) :**

Reporting Log
Group .....

Date	Time	Incident	Action taken		Incident Reported by	Signature
			What?	By whom?		

Response to Risk Flowchart

Response to and Reporting of an E-safety Incident of Concern