Holy Trinity Roman Catholic Academy Boundary Road
Newark NG24 4AU

E-SAFETY AND ACCEPTABLE USE POLICY

Holy Trinity Roman Catholic Academy Boundary Road Newark NG24 4AU

POLICIES & PROCEDURES
DOCUMENT CONTROL SYSTEM

Controlled Document reference:

Document Title: **E-SAFETY POLICY**

Date of creation: September 2016

Date of last review: September 2023

Scheduled review date: September 2025

Holy Trinity Catholic Voluntary Academy
Mission Statement

“In every child there is a space only God can fill”

St Thomas Aquinas

At our school we continually strive to develop the full potential of the school community in an environment permeated by the Catholic Faith and promoting Gospel values.

At the heart of our mission is the family, school and parish, each supporting and working in mutual co-operation for the benefit of the children.

We are seeking to enrich the lives entrusted in our care through a broad and balanced curriculum designed to meet the needs of each pupil.

The school provides opportunities for young children to develop spiritually, morally, intellectually, physically and emotionally, and share their qualities, abilities and ambitions thus fulfilling individual potential.

As a worshipping community we respect all people and create a loving, caring atmosphere which overflows into an ethos of warmth and welcome towards parents, parish and the local community

Holy Trinity Catholic Voluntary Academy
E-Safety Policy

Introduction

At Holy Trinity Catholic Voluntary Academy we provide a diverse, balanced and relevant approach to the use of technology, where the children are encouraged to maximise the benefits and opportunities that technology has to offer. When delivering the school curriculum, teachers will plan to integrate the use of communications technology such as web-based resources, e-mail and mobile learning tablet devices to enhance pupils' learning. These skills are vital to access life-long learning and employment. Young people have access to the Internet via a range of devices from many places. Holy Trinity Catholic Voluntary Academy has a number of measures to help ensure that curriculum use is safe and appropriate in school, however, access out of school does not always provide these same measures and has a range of risks associated with its use. This policy is designed to ensure pupils' e-safety both in and out of the school environment. In order to achieve this, we will ensure that the children learn in an environment where security measures are balanced appropriately with the need to learn effectively, and will equip the children with the necessary skills and knowledge to use all technologies appropriately and responsibly, helping them to recognise risks and how to deal with these both in and out of school.

E-safety depends on staff, governors, parents and the pupils themselves taking responsibility for the use of the Internet and other communication technologies such as mobile devices. There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant at all times when using the internet.

This policy makes links with the following policies: Child Protection Policy, Behaviour Management Policy, Anti-Bullying Policy, GDPR policies and guidance.

This policy should be read in conjunction with OLOL Online Safety Policy.

1. The School's Network

Full information can be found in the Trust's IT Security Policy

1.1 System network provider

The school has an ICT suite containing PCs and a laptop trolley. Teaching staff have access to a laptop and an ipad that can be used off site. All devices are linked to the school's network which contains recommended filtering systems and virus protection.

1.2 Passwords

* All staff have their own username and passwords via which to access their emails and use a teacher password to assess the network
* Passwords are changed regularly
* Children have their own class logins which gives access to only certain areas of the system
* Children and adults are aware of the need to keep passwords secure
* Children use class logins only – staff do not login for children's use with their own login details

2. Internet Safety

2.1 Why is Internet use important?

The Internet is an essential element in 21st century life for education, business and social interaction. Holy Trinity Catholic Voluntary Academy believes it has a duty to provide pupils with quality Internet access as part of their learning experience.

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

2.2 How will Internet use enhance learning?

The school Internet access is designed expressly for educational use and includes filtering appropriate to the age of pupils. Access to the internet enhances all aspects of learning across all curriculum areas.

2.3 How will Internet access be authorised?

* Internet access will only be granted through the school's server
* At the EYFS and KS1 access to the Internet will be by teacher or adult demonstration in the first instance, and alongside the school's internet safety rules and e-safety curriculum. Pupils may access certain sites as directed by the teacher where appropriate under supervision.
* At KS2 Internet access will be granted to a whole class as part of the scheme of work after regular reminders of the rules for responsible Internet use
* Parents will be informed that pupils will be provided with supervised Internet Access (see Appendix 2 which will be available on the school website)
* The school's e-safety curriculum will support teaching pupils' safe internet use

2.4 How will the school ensure that the Internet use provides effective learning?

* Filtering systems are built into all school devices to protect unsuitable content appearing on screens
* Prior to use, all pupils will be reminded of the school's Internet Safety Rules
* During curriculum time, teachers will inform pupils which websites they are allowed to access or which key words they are allowed to use in internet search engines; all of which will be monitored closely. It may be appropriate for older children to have access to the open internet, but access will be purpose driven linked to a particular theme of study; QR codes may also be used to direct children to appropriate websites for research purposes
* When using ipads, children will be requested to keep the ipad flat on the table to facilitate close supervision
* Pupils will not have free access to the internet during any Golden Time or at the school Breakfast Club or After School Clubs, but where appropriate, will be directed to particular sites that are deemed suitable by staff, particular search words or to specific APPs that they may use
* Any children not complying with these measures will not be allowed to use the internet for a given period of time
* If staff or pupils do discover any unsuitable material, the URL (address) and content must be reported to the ICT Manager and the school's IT Technician
* Parents of the children involved will be notified immediately
* Nominated persons (IT technician) will be responsible for permitting and denying additional websites as requested by colleagues.
* Pupils will learn appropriate Internet use and be given clear objectives for this
* Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
* The school's Internet Rules (Acceptable Use Policy) will be shared regularly with pupils and displayed in each classroom and the ICT suite, and any location where ipads, laptops or computers are being used

2.5 How will the risks be assessed?

* In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
* Methods to identify, assess and minimise risks will be reviewed regularly.
* The Headteacher, IT Leader and Designated Safeguarding Lead will ensure that this policy is implemented and compliance with the policy monitored.

3. The School Website

3.1 Managing and evaluating the School Website content

* The point of contact on the website is the school address, school e-mail and telephone number
* The content of information placed on the website will be verified by the Head Teacher
* Website photographs that include pupils will be selected carefully and will not enable individual pupils to be identified by name
* Written permission from parents or carers will be obtained before photographs of pupils are published on the school website, as per the sample appendix letter

4. Staff Acceptable Use

4.1 EMAIL

All staff are issued with a school email address for school use. The following is requested of staff:

1. **Check** your mail regularly, and reply promptly where appropriate.
2. **Develop** an orderly filing system for those email messages you wish to keep; delete unwanted ones to conserve disk space.
3. **Keep** email messages fairly brief. Remember it will usually be read on a computer screen.
4. **Try** to use the 'subject' field to convey the subject of the email, and don't use the subject line to convey the entire message.
5. **Remember** humour and satire, are easily misinterpreted.
6. Email is not guaranteed to be private; people other than the person to whom it's addressed may see your message; i.e. recognise that anyone along the chain of distribution could get to see what you have said, and it might even end up in someone else's hands.
7. Remember not to type the whole message in capital letters
8. School email addresses should **NOT** be used for making online purchases for personal use. When online purchases are required for school purposes please consult the school's Finance Manager, and ensure that you have received the required authorisation from the Head or Deputy Headteacher.

4.2 STAFF INTERNET USE:
Refer to the Trust's Staff Acceptable Use policy for further information.
In summary:
The staff at Holy Trinity Catholic Voluntary Academy will not:
* access offensive websites or download offensive material.
* place inappropriate material onto the Internet.
* disregard their responsibilities for security and confidentiality.

* download files that will adversely affect the security of the school network.
* access the files of others without permission
* update web pages or use pictures or text that can identify the school on personal sites, blog, social networks etc without the permission of the Head teacher.
*refer to the school by name on social networking sites

4.3 SOCIAL NETWORKING

*Staff's personal social networking settings will be kept secure
* Comments made about the school, pupils or other members of staff are not appropriate, and content posted online should not: bring the school or anyone associated with the school into disrepute, lead to parental complaints or be deemed derogatory towards the school and / or its employees, pupils or parents/carers. Any such comments made by staff will be dealt with via either the school's Disciplinary or Grievance policy where appropriate
* Staff may not accept pupils or former pupils as friends, and must not give personal contact details to pupils or parents
* Inappropriate comments made by pupils regarding the staff or children could be construed as cyber bullying and will be dealt with via the school's Behaviour Management policy or Anti-Bullying Policy where appropriate

4.4 STAFF MOBILE PHONES:

Staff mobile phones may only be used in emergencies, on educational visits to make contact with the school, parents etc or during break times, lunch times and at the beginning and end of the school day, where calls or access to the internet via these is granted
* During contact with children, mobile devices should remain on silent unless in emergency situations that have been agreed in advance – all staff including volunteers and visitors should arrange for the school's telephone number to be available to family or friends in an emergency
* Staff's personal mobile devices or cameras will not be used for taking photographs of children
* The school's Volunteer Handbook makes this requirement clear to all students and volunteers in the school

5. On-line communications and social networking.
* The use of online social networking sites is not permitted in school
* It is recognised that despite pupils of primary aged not being eligible to use social networking sites such as Facebook, many children will have access to this at home. Pupils will be taught how to keep personal information safe when using online services, and how to keep themselves safe when playing games online etc.
* The school does not take any responsibility for actions taken by pupils when using such sites at home; however any issues brought into the school will be dealt with via the school's behaviour management policy and the e-safety curriculum will ensure that children are taught ways to keep themselves when using devices and internet sites out of school

6. Children's Use of Mobile technologies

6.1 Safe use of ipads
* Appropriate use of mobile devices such as ipads will be taught to pupils as part of their e-safety programme, and expectations for use will be set out by class teachers at the beginning of the year
* All ipads have suitable filtering systems and internet access is granted via the school's network
* Children are reminded of the Internet Safety Rules / Acceptable Use Policy prior to using these devices

* When using ipads, unless taking photos or recording, children will be requested to keep the ipad flat on the table to facilitate closer supervision
* Ipads and Laptops are stored in the ICT suite which is locked every evening. Teachers are responsible for returning these to the relevant trolley at the end of the session or school day. This is monitored by the ICT Leader
* Any school ipads or laptops taken out of school for staff use are signed out and in again on return

6.2 Personal Devices

* Pupil mobile phones are not permitted within the school. In the event of a child bringing their device into school, this will be locked away securely and returned to the child on their departure. School staff cannot take responsibility for lost or damaged mobile phones
* Parents attending school events are given permission to take photographs or record their children during assemblies or productions; however, they are requested to sign in on doing so and to support the school's policy in not uploading any images onto the internet
* All staff are responsible for the monitoring of this part of the policy – any behaviour related to this which causes concern from a volunteer, visitor, parent, child or member of staff is to be reported to the Designated Teacher for Safeguarding and the Head Teacher immediately

6.3 Use of storage facilities

The school uses the One Drive to store work, along with staff individual laptop storage and the Staffroom Drive.

6.4 Removable media

* Each class teacher has a school ipad and laptop, which can be removed from the premises. These are all password protected and staff are aware of the Acceptable Use Policy and not divulging passwords to others
* Staff's personal devices are not to be used to download data from school systems

6.5 Use of cameras, recording devices and use of Children's Photographs

Holy Trinity Catholic Voluntary Academy needs and welcomes positive publicity. Children's photographs add colour, life and interest to photographs of school activities and initiatives. Making use of photographs in school publicity materials can increase pupil motivation and staff morale and help parents and the local community identify and celebrate the school's achievements.

However, photographs are used in a responsible way. Holy Trinity Catholic Voluntary Academy respects young people's and parents' rights of privacy and is aware of potential child protection issues.

We balance potential risks against the advantages of promoting the school in a colourful and attractive way.

Child protection issues

Risk occurs when individual pupils can be identified in photographs. Providing the name and photograph of a pupil in a publication or on a website allows for the possibility of people outside the school identifying and then contacting pupils directly. In order to address this, children's names will not appear with their photo on the internet. The Head teacher will decide whether publication of a photograph might pose a risk to a child.

Data Protection

Photographs and video images of pupils and staff are classed as personal data under the terms of the GDPR regulations May 2018. Using such images for school publicity purposes will require the consent of either the individual concerned or in the case of pupils, their legal guardians. This means that Holy Trinity Catholic Voluntary Academy will not display images of pupils or staff on websites, in publications or in a public place without such consent. Contact details for parents and other personal information on computer systems are stored confidentially under the data protection act, and not disclosed to other parties without prior permission.

Permission will be obtained from all the people who will appear in a photograph, video or webcam image before we record the footage. That means adults as well as children.

Taking images at an event attended by large crowds, is regarded as a public area so it is not necessary to get the permission of everyone in a crowd shot. Children in the foreground are also considered to be in a public area, and if any of these children are identifiable in the photograph, the school will check its consent forms prior to any publication.

Further Data Protection information can be found in the Trust's GDPR policy.

Appropriate use of images

The School will:

- Only use images of children in suitable dress to reduce the risk of inappropriate use.
- Ensure that no photographs are taken at the swimming pool
- Never use an image of a child who is subject to a court order
- Make sure images are stored securely and used only by those authorised to do so
- Secure parental consent.

Websites

The school is aware of the potential risk of inappropriate images because of the lack of control you have over who might see the image and the wide extent of misuse of the internet by certain people.

Our consent form explicitly includes publication on the internet. When photos of pupils are used on our websites, names of those pupils would not be included.

Newspapers

The use of photographs in newspapers is already subject to strict guidelines. The Press Complaints Commission's Code of Practice states that:

- **Journalists must not interview or photograph a child under the age of 16 on subjects involving the welfare of the child or any other child in the absence of or without the consent of a parent or other adult who is responsible for the children.**
- **Pupils must not be approached or photographed while at school without the permission of the school authorities.**

Filming events

The school recognizes that parents or other spectators may want to photograph or video at an event such as a sports day or arts performance. This is a valuable part of school life and can be very rewarding for both the family and school. However, we have a duty to safeguard our children, therefore prior to any filming taking place at such events, the school will request that parents do not put any images on the internet, including social networking sites.

If children or parents have any concerns about inappropriate or intrusive photography, they should report them to the school who will deal with them in the same manner as any other child protection concern.

If schools or parents have concerns regarding the use of filmed images by TV companies, they should contact the Office of Communications (Ofcom).

Parental consent

Consent for photographs to be taken and used along with other parental permissions is part of our registration process when a child starts at our school. Consent is requested for the duration of the child's time at the school and avoids the need to ask for parental consent on each and every occasion that photographs are taken.

When children have left the school, the consent forms are discarded securely. Consent from teachers and any other adults who may appear in the photograph or video will be gained on an as necessary basis.

Use of Cameras

In addition to the use of photographs for public use, the school also recognizes its duty to keep children safe by means of ensuring that the device used to take the photographs is safe:

Children's use of cameras:
If children take any photographs of other children as part of the curriculum, they should use only one of the school's cameras or ipads and any photographs will be downloaded/deleted after use.

Children leaving the school may with permission, take photographs of their friends, but this permission will always be sought prior to taking. Staff will remain vigilant and ensure that children whose parents have refused their child to have their picture taken are not included in this, unless special permission is granted by parents prior to doing so.

Staff and Governors use of cameras:

Staff and Governors must use only one of the school's cameras or ipads to take photographs of children and any photographs should be downloaded/deleted after use**.** Staff and governors MUST NOT use any other device, including their own personal camera, ipad or mobile phone to take photographs of children, unless they are a parent of a child at the school. The responsibility for the downloading /printing of photographs lies with the member of staff taking the photograph.

All photographs or films taken using school cameras or ipads and should be downloaded and removed from that device as soon as possible – staff taking the photographs are responsible for downloading and deleting from the device, to secure safely on the school's main system

Equal Opportunities

This is an issue that concerns all children in schools but particular sensitivity is required when dealing with photographs of children with special educational needs. Schools should also consider whether the images they use represent the broad range of young people in the school. Photographs should include both boys and girls, pupils from minority ethnic communities and young people with disabilities where appropriate

8. Communication with Parents

In order to communicate effectively with parents, the school uses:

- Text Round as a facility to make contact with parents. The facility does not allow all recipients access to other recipients contact details.
- Email through SIMS, set up so all recipients cannot access others' contact details
- Class Dojo – messaging facility to all parents for general messages either via the Whole School or Classes and individual messages directly to parents

9. Introducing the Policy to Pupils

* Rules for Internet access / (Acceptable User Policy) will be posted in all rooms where computers and mobile devices such as ipads are used
* E-safety will be discussed with pupils regularly and reminders given when devices are in use
* Instruction on responsible and safe use should precede Internet access.
* Pupils will be informed that Internet use will be monitored.

10. E-Safety Curriculum

* The E-safety curriculum forms part of the school's PSHE curriculum and links are also made with work carried out in RE Lessons and Enrichment Week activities such as Healthy Week and Anti-Bullying Week. The school uses its Computing Scheme of Work which is progressive across the school from the EYFS to Year 6, covering age appropriate material to help children make informed choices and protect themselves in matters concerning e-safety both at school and out of the school environment. The e-safety message is also reinforced throughout the year via assemblies, activities during Internet Safety Day, class and school council discussions etc. Pupil and parent e-safety training is offered annually and staff training is also updated on an annual basis.

11. Dealing with incidents

* Sanctions for pupil mis-behaviour regarding any e-safety issues will be dealt with in line with either the schools' Behaviour Management Policy or the Anti-Bullying Policy. These may be summarised as follows, but this list is not exhaustive:

Incident	**Procedure or Sanction**
Accidental access to inappropriate images	• Children should minimise the webpage and turn the monitor off and tell the adult in charge • The adult in charge should enter the details in the Incident Log held in the School Office and report it to the ICT Leader / IT Technician / Head Teacher • Persistent 'accidental offenders' will receive sanctions in line with the school's Behaviour Policy
Deliberate searching for inappropriate images Using the internet in an inappropriate way Cyber Bullying in school – unkind emails etc Cyber Bullying out of school	• Inform ICT Leader and Head Teacher or SLT • Record in Incident Log • Raise awareness of AUP / Internet Rules with class – refer to e-safety curriculum • Deal with the incident in line with the school's Behaviour Management Policy

* Any suspected illegal material or activity must be brought to the immediate attention of the Head Teacher to must refer this to external authorities. The Head Teacher will never personally investigate, interfere with or share evidence in suspected illegal matters

11.1 Cyber Bullying

* Teaching children about Cyber-Bullying will form part of the school's e-safety and anti-bullying curriculum, which forms part of the school's PSHE curriculum. Assemblies, Internet Safety Day, Anti-bullying Weeks, parental training, training for pupils and external visitors will also reinforce the school's message about cyber bullying, what it might look like, what children should do and how this can be prevented.

11.2 Reporting Abuse

Children will be taught how to report any acts of unkindness/ cyber bullying etc by telling an adult in school, in the understanding that all allegations will be taken seriously and investigated thoroughly in line with this policy and the Behaviour Management and Anti-Bullying Policies. They will also be informed of the methods of reporting abuse online when using the internet out of school via the Report Abuse icon.

12. Parents and E-Safety

* Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school Website, which has a specific page regarding e-safety
*Regular information will be provided to parents to help ensure that this policy is used appropriately both within school and home.
* Internet issues will be handled sensitively to inform parents without undue alarm.
* A partnership approach with parents will be encouraged. This will include an opportunity for parents to access relevant training and could include demonstrations, practical sessions and suggestions for safe Internet use at home.
* All parents will receive support information as and when appropriate, for example via the CEOP website

13. Consulting with stakeholders and their inclusion in the E-safety Policy

* All staff including teachers, teaching assistants and support staff, will be involved with the implementation and review of this policy and its importance
* Parents and pupils will also be consulted regarding this policy
* Staff and pupils should also be aware that Internet traffic is monitored and can be traced to the individual user.
* Staff development in safe and responsible Internet use and on the school Internet policy will be provided annually
* The school's Induction policy for new staff includes reference to this policy and updated training

14. How will complaints be handled?

* Any complaints regarding e-safety will be handled in line with the school's Complaints Policy
* Any complaint about staff misuse must be referred to the Headteacher.
* Parents and pupils will need to work in partnership with staff to resolve issues.
* There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

15. Responsibility

* All staff are responsible for implementing this policy and for recording and responding to all incidents which refer to e-safety, which usually will fall under the Behaviour Management Policy. These should

be reported to the ICT Leader and Head Teacher, or SLT member. The Head Teacher is responsible for monitoring any e-safety related incidents, and the governing body will monitor these in line with their monitoring cycle. Prevention of e-safety and cyber bullying incidents are dealt with in the Behaviour Management and Anti-Bullying Policies.

16. Policy review

This policy will be reviewed annually by Local Governing Body.

HOLY TRINITY CATHOLIC VOLUNTARY ACADEMY

E-SAFETY ACCEPTABLE USE POLICY
CHILDREN'S RULES FOR RESPONSIBLE INTERNET USE

These rules will keep you safe and help us be fair to others:

1 I will only access the system with the login and password that I have been given; I will not tell anyone my own personal passwords

2 I will not access other people's files;

3 I will only use ICT in school for schoolwork and homework;

4 I will not bring mobile devices into school unless I have been given permission or specifically asked by my teacher; (Y5/6 – if I bring my mobile phone into school, I will hand it in to my teacher at the beginning of the school day. It will not be left in my bag or accessed during the school day)

5 I will ask permission from a member of staff before using the Internet, and will not deliberately look for or access inappropriate websites;

6 I will not give my home address or telephone number, or arrange to meet someone, unless my parent, carer or teacher has given permission;

7 If I accidentally find any material on the internet which is inappropriate or if I receive messages from people who I do not know or which upset me, I will report this immediately to my teacher. I understand this report would be confidential and would help protect other pupils and myself;

8 I will not attempt to download or install anything onto the school network unless asked to do so by my teacher

9 I understand that the school may check my computer files and may monitor the Internet sites that I visit. I understand that my parents may be contacted if a member of staff is concerned about my e-safety.

10 I understand that if I do not follow these Internet Safety Rules I will receive sanctions in line with the School's Behaviour Management Policy

Holy Trinity Catholic Voluntary Academy, a Voluntary Academy

E-Safety Information for Parents

- ✓ At Holy Trinity Catholic Voluntary Academy, we expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.

- ✓ Pupils using the Internet are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher.

- ✓ Pupils are expected not to use any rude language in their email communications and contact only people they know or those the teacher has approved. It is forbidden to be involved in sending chain letters.

- ✓ Pupils must ask permission before accessing the Internet

- ✓ Pupils should not access other people's files unless permission has been given.

- ✓ Computers should only be used for schoolwork and homework unless permission has been granted otherwise.

- ✓ No files may be downloaded to the computer or ipad from the Internet.

- ✓ No mobile devices should be brought in from home for use in school.

- ✓ Homework completed at home may be brought in on USB sticks but this will have to be virus scanned by the class teacher before use.

- ✓ Personal printing is not allowed on our network for cost reasons (e.g. pictures of pop groups/cartoon characters).

- ✓ No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.

- ✓ Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources.