



# St Thomas of Canterbury Catholic Primary School

Where every child is special

## Online Safety and Cyber Policy

Policy compiled by:

Amy Grove, Online Safety Leader

Date of last review:

Spring 2018

Review Date:

Spring 2019

The  
**CHILD**



The whole  
**CHILD**

Nothing but  
the **CHILD**

### OUR SHARED VISION

*Every child* at St Thomas of Canterbury is special and will achieve their full potential academically, socially, spiritually and emotionally through the provision of a loving community and rich and varied learning opportunities and the highest quality teaching and learning.

*Every staff member* at St Thomas of Canterbury will feel valued and enabled to provide the opportunities that we want for our children and to do so as part of a loving community which has the highest expectations of and for all.

*Every Governor* at St Thomas of Canterbury will feel valued and enabled to act as a critical friend to the School and to be accountable for the School's strategy. They will play a visible role supporting all children, their parents and staff at School and in the wider community, to provide the best environment possible for learning and spiritual growth.

### OUR MISSION STATEMENT

*God's love is at the heart of our Catholic School family.*

*We show this in our respect, kindness and love for others and by treating other people as we wish to be treated ourselves.*

*We will encourage everyone to be the best that we can be.*

### OUR AIMS

- To guide our children to grow in the love of God and build relationships that will enable them to make a positive contribution to the School and society.
- To develop an exciting, challenging and creative curriculum that produces confident and successful learners who are the best that they can be.
- To develop high quality learning that enables every child to flourish, to discover their talents and be lifelong learners.
- To establish a teaching and learning environment that encourages everyone to enjoy, to achieve, to be inclusive, to be healthy, and to stay safe.
- To nurture a strong partnership between home and School.
- To have respect and understanding for our School, our community and our world, helping our children to become responsible citizens and good role models.



## **OUR GOLDEN RULE**

We treat others as we would like to be treated

### **Aims**

The aim of this policy is to make clear the procedure for the use of the Internet by all members, including pupils, staff, parents, governors and visitors of St. Thomas of Canterbury School. The policy outlines the reasons for the use of the Internet and the simple guidelines, which must be followed by all in order to maintain a high level of security, privacy and safety. Any guidelines which are not followed will be reported to the Online Safety Leader, recorded and further action will be taken.

### **Online Safety**

The school has an appointed Online Safety Leader who attends annual CEOP (Child Exploitation and Online Protection) training and obtains a validated training certificate as well as keeping up to date with Online Safety issues and documentation. The Online Safety Leader is also part of the Online Safety Committee which further consists of the Headteacher who is a Designated Safeguarding Lead and the Safeguarding Governor. This Online Safety Policy has been written by the school, building on best practice and Local Authority and government guidance. The Online Safety Policy is reviewed by all staff and governors annually.

### **Introduction**

The Internet is a valuable tool within schools and is an ever increasing source of information for all curriculum areas. It is an essential element in 21st century life for education, business and social interaction.

We, as a school, have a duty to provide pupils with quality Internet access as a part of their learning experience. Therefore the general use of the Internet is increasing throughout the school from Early Years Foundation Stage (EYFS) to the end of Key Stage 2 as pupils are given the opportunity to clarify, analyse and understand information they have studied.

The Internet is also an area that as a school we must ensure is as safe for the pupils to use as possible. As a result we need to set out strict rules, which will be followed by all members of St. Thomas of Canterbury using the School PCs or Laptops whilst on school premises, including Breakfast Club, After School Club, Animation and Micro:Bit Club and Study Club.

These rules will be enforced primarily by all staff but pupils also have a responsibility to adhere to these rules as well as reporting any misuse.

All staff and governors have signed an Acceptable Use Policy in agreement with the school's policy (see Appendix 4). Visitors to the school agree to the Acceptable Use Policy upon their signing in.

### **Teaching and Learning**

Internet use is part of the statutory curriculum and a necessary tool for staff and pupils. Pupils will be taught what Internet Use is acceptable, and what is not, and given clear objectives for Internet use as outlined in our 'Cyber Contract'. We have two Cyber Contracts, both discussed and written by the pupils through School Council and staff: one for EYFS and Key Stage 1 and one for Key Stage 2. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be shown how to publish and present information appropriately to a wider audience. All pupils will only have access to the internet in school under adult supervision.

Online Safety is taught half-termly to all pupils and further reinforced with assemblies throughout the year. St Thomas of Canterbury participates in the annual Safer Internet Day and encourages



pupils to be actively involved in their learning. Should an incident or issue arise, further discussion and teaching will be had with the involved class or year group or phase as appropriate.

### **Pupils will be taught how to evaluate Internet content**

The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law. Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector and are encouraged always to tell a trusted adult.

### **Managing Internet Access:**

#### **Information system security**

School ICT systems security is reviewed regularly by the ICT technician/Computing Leader with support from RM Safetynet. The virus protection software updates to the server daily and the technician is able to see if any problems occur on a weekly basis. Any filtering concerns from staff or pupils should be brought to the attention of the ICT/ Computing Leader. Security strategies and filtering/monitoring routines are guided by RM Safetynet and Babcock.

#### **E-mail**

Pupils and staff may only use approved e-mail accounts on the school system and must immediately tell a teacher if they receive an offensive e-mail and attachments should not be opened unless the author is known. Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone. Staff to pupil email communication must only take place via a school email address in the context of a specific lesson and will be monitored by staff and the ICT/Computing Leader. Emails accessed at school are filtered through the 'Safety Net Cloud Filtering'; any links deemed unsuitable will be automatically blocked. Any inappropriate emails sent will result in the email account being closed.

#### **Published content and the school web site**

The contact details on the Web site will only be the school address, e-mail and telephone number. Staff or pupils personal information will not be published. Confidentiality of staff and pupils must be maintained at all times.

#### **Publishing pupil's images and work**

Photographs that include pupils will be selected carefully. The school will look to seek to use group photographs rather than full-face photos of individual pupils. Pupils' full names will not be used on the Website, in association with photographs. Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website when the pupils join the school. A record is kept by class teachers and in the school office. Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

#### **Social networking**

The school will **NOT** allow access to social networking sites, such as Facebook and Twitter and will educate pupils in their safe use outside of school e.g. use of passwords and usernames and abiding by age restrictions. Pupils will be advised never to give out personal details of any kind which may identify them or their location. Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils and will be reminded of the age restrictions on common sites. Pupils will be advised to use nicknames and avatars when using age appropriate social networking sites.



## **Managing filtering**

The school will work to ensure systems to protect pupils are reviewed and improved regularly. If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety Leader, Headteacher or ICT Technician/Computing Leader immediately in person or via email. The ICT technician, will ensure that regular checks are made to ensure that the filtering methods used are appropriate, effective and reasonable.

## **Managing emerging technologies**

Emerging technologies will be examined for educational benefit and discussions will be carried out before use in school is allowed. EYFS currently use iPads to collate information about the children's progress to inform their assessments.

## **Protecting personal data**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. Once the new GDPR legislation comes into effect from May 2018 further guidance and procedures will be implemented with all staff.

## **Assessing risks**

The school will take all reasonable precautions to prevent access to inappropriate material. Members of staff are expected to remain vigilant and filtering is in place. Appropriate filtering and monitoring (physical and Internet and Web Access) is in place, RM blocks websites deemed unsuitable but not so much as to restrict children's learning. Should a member of staff require a particular website for teaching purposes, then a request must be sent to the ICT Technician/Computing Leader who will investigate, with the Online Safety Leader, the website for its suitability. If approved, the website will be unblocked and kept on a record log.

However, due to the international scale and linked 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. The school will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective. Any new software or online facility is always assessed and fully researched by the ICT technician/Computing Lead and Online Safety Leader, including consulting with other schools, before it is made available to the pupils.

## **Handling Online Safety complaints**

Complaints of Internet misuse will be dealt with by the Online Safety Committee. Any complaint about staff misuse must be referred to the Headteacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. Pupils and parents will be informed of the complaints procedure. See Appendix 1. All incidents will be recorded by the school.

## **Misuse of the Internet**

This would be considered a breach of school policy. Any misuse of the Internet by pupils will lead to consequences including a ban from the use of the Internet at school. Any misuse of the Internet by staff will be dealt with by the Headteacher. See Appendix 1. All incidents will be recorded by the school using the behaviour log system. The use of the Internet is checked on a weekly basis by the ICT Technician and a record kept.

## **Introducing the Online Safety policy to pupils**

Appropriate elements of the Online Safety policy will be shared with pupils through the 'Responsible Cyber User Contract'. This contract has been written in consultation with our School Council and there is a contract for EYFS/KS1 (Appendix 2) and another for KS2 (Appendix 3). Pupils regularly review this contract with their class teacher. These will be on display in the Computing Suite. Pupils



will be informed that network and Internet use will be monitored. Pupils will learn about Online Safety each half term in Computing and through special assemblies and in PSHCE (Personal, Social, Health and Citizenship Education).

### **Staff and the Online Safety policy**

All staff will have read and contributed to the School Online Safety Policy and its importance explained. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential and staff should also refer to their staff handbook for further information regarding professional conduct. At St. Thomas' we respect and trust our staff to use the Internet sensibly.

The ever increasing use of technology is vital to our everyday teaching and learning. Staff should refer to the Acceptable User Policy and ICT Code of Conduct for further information about responsible use of technology at St. Thomas of Canterbury.

### **Staff Use of Social Media Sites outside of school**

Whilst staff are permitted to use social media sites, the nature of the Internet means that such sites can leave us vulnerable if we fail to observe a few simple precautions. We need to remember we have a professional image to uphold and how we conduct ourselves online holds no exceptions. This advice comes from a variety of sources, including the DfE, Babcock and experiences of other school staff. Staff should read the staff handbook for further information.

### **Mobile Technology**

Personal devices including phones and tablets may be brought into school by staff and governors. It is important to remember that when these mobile devices are brought in they should be connected to the school internet network; the users have a responsibility to comply with this Online Safety Policy and guidelines. Such technology should only be used for school related purposes and not for personal use.

Staff and governors must not store images of pupils or pupil personal data on their personal devices. Staff and governors are solely responsible for their own personal devices. The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business. Any issue should be immediately reported to the Online Safety Co-coordinator.

### **Parents and Online Safety**

Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school website. Parents and carers will be asked to attend an Online Safety Information Meeting when their child(ren) enrolls. It is the responsibility of parents to support their pupils in safe internet use included as a statement on the home school agreement and to sign the 'Responsible Cyber User Contract' with their child(ren) – see appendix 2 and 3. This contract shows they will agree to follow the school rules for safe internet use. Up-to-date information and advice are sent out to parents when appropriate.

### **Further Internet Guidance at School**

1. It is the responsibility of parents to support their pupils in safe internet use included as a statement on the home school agreement and to sign the 'Cyber Contract' with their child(ren) annually
2. Pupils are only allowed to use links given by the school
3. The use of 'Search Engines' is NOT permitted, unless in the presence of a member of staff.
4. The 'Search Engines' used by the pupils at St. Thomas of Canterbury School all offer a filtered list of links.

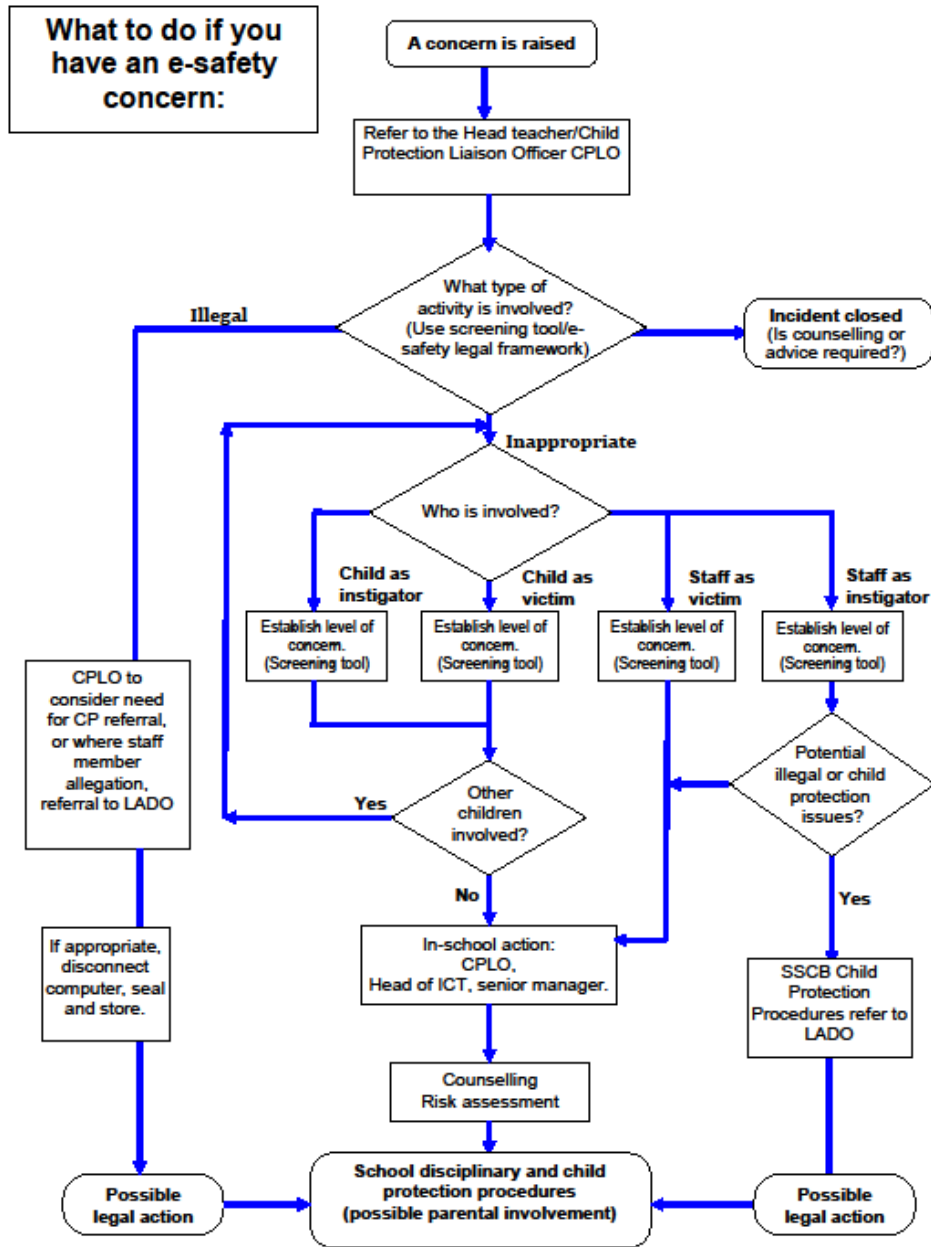


5. All Internet access at St. Thomas of Canterbury School is filtered through a proxy server to screen any undesirable sites at source therefore any child finding themselves uncomfortable or upset by anything they discover on the Internet should report it to a member of staff immediately
6. Pupils will only be referred to by their first name on our web site
7. Any images of pupils will not be labelled with their names. Written permission from parents/carers will be obtained before photographs of pupils are published on the school web site or Learning Platform
8. No close up images of our pupils will be available online; images shown on the school's website only appear with parental permission
9. Pupils will never reveal their home addresses or telephone numbers on the web
10. All E-mails to classes will be monitored by the class teacher
11. Pupils do not have individual email addresses and will not be allowed to check their private addresses as this can lead to potential viruses on the system
12. Pupils are only allowed to use regulated educational chat environments. This will be supervised and the importance of chat room safety emphasised
13. Pupils are not allowed to bring into school external storage media such as CDs, memory sticks or other such devices, and attach these to a School PC with teacher approval if absolutely necessary
14. Teachers monitor pupils' files and internet sites that they visit
15. Teachers will monitor appropriate use of the computers at all times to ensure that the pupils are behaving sensibly and to ensure that no form of cyber bullying can occur

*This policy of St Thomas of Canterbury School upholds the school's ethos and Mission Statement. It must be read in conjunction with and implemented in accordance to the school's policies for ICT/Computing, Health & Safety, Equal Opportunities, Inclusion and Safeguarding. Copies of these policies are available from the school office website.*














Appendix 1:





**Appendix 2: EYFS and KS1 Cyber Contract**

These rules will help us to be fair to others and keep everyone safe. Everyone at St Thomas of Canterbury is expected to follow these rules. We use the school computers and Internet for our learning. We will not bring in any mobile devices into school unless directed by a teacher.

-  I will only use the Internet at school with an adult.
-  I will only click on the buttons or links when I know what they do.
-  When I use the Internet, I will not give out my personal information: full name, passwords, my home address or phone number, age, what school I go to.
-  I will never arrange to meet someone I don't know.
-  I will also not give out anyone else's personal information.
-  I will use a nickname online.
-  I will write polite and friendly messages and comments online following our Golden Rules.
-  If I see anything I do not like, I will tell an adult straight away.
-  I will not deliberately delete other people's work or comments on the home or school computer including the use of the Learning Platform.
-  I understand that if I deliberately break these rules, I will be stopped from using the Internet for weeks/term or until the teacher thinks I can use it sensibly.
-  If I accidentally break any of these rules I will tell a teacher immediately.

**Child's name:** .....

**Signed:**      **Child:** .....

**Parent:** .....
















**Date:** .....





**Appendix 3: KS2 Cyber Contract**

These rules will help us to be fair to others and keep everyone safe. Everyone at St Thomas of Canterbury is expected to follow these rules. We use the school computers and Internet for our learning. We will not bring in any mobile devices into school unless directed by a teacher.

-  I will only use the Internet at school when a responsible adult is present.
-  When using the Internet or email, I will not give out my personal information: full name, passwords, my home address or phone number, age, school details, email address or arrange to meet someone we don't know. I will also not give out anyone else's personal information.
-  I will use a nickname when completing activities online.
-  I will only use websites and games online with a responsible adult's permission.
-  I will send polite, friendly and sensible messages with a responsible adult's permission following our Golden Rules. If we wouldn't say it to someone, we wouldn't write it on the Internet or in an email.
-  I will only e-mail or open emails from people I know, with a responsible adult's approval.
-  I will not chat to anyone I don't know online at any time.
-  I will be aware of what words to type in for a search for images.
-  If I see anything I am unhappy with, anything that concerns me or I receive messages I do not like, I will tell an adult immediately.
-  I understand that the school may check my computer files and may monitor the Internet sites I visit.
-  I will only use any DVDs or memory stick at school with a responsible adult's permission.
-  I will not deliberately delete other people's work or comments on the home or school computer including the use of the Learning Platform.
-  I will not go into the control panel without permission.
-  I understand that if I deliberately break these rules, I will be stopped from using the Internet for weeks/term or until the teacher thinks I can use it sensibly.
-  If I accidentally break any of these rules I will tell a teacher immediately.

**Child's name:** .....

**Signed:**           **Child:** .....


















**Parent:** .....

**Date:** .....



## **Appendix 4: Acceptable Use Policy and ICT Code of Conduct**

ICT and the related technologies such as email, the Internet and mobile devices are an expected part of our daily working life in School. All staff need to be aware of their professional responsibilities when using any form of ICT. Any concerns or clarification should be discussed with the E-safety coordinator and/or the Senior Leadership Team.

-  ICT includes a wide range of systems, including mobile phones, tablets, digital cameras, email, and that ICT use may also include personal ICT devices when used for School business.
-  It is a criminal offence to use a School ICT system for a purpose not permitted by its owner.
-  The School's email/Internet/Learning Platform and any related technologies must only be used for professional purposes, or for uses deemed 'reasonable' by the Head or Governing Body.
-  All staff must comply with the ICT system security and not disclose any passwords provided by the School or other related authorities.
-  All staff are responsible for all activity carried out under their username.
-  All staff must ensure that all electronic communications with pupils and staff are compatible with their professional role and only use the approved, secure email system(s) for any School business.
-  Staff must ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in School, taken off the School premises or accessed remotely. Personal data can only be taken out of School or accessed remotely when authorised by the Head or Governing Body.
-  Staff must not install any hardware or software without permission.
-  Staff must not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
-  Images of pupils and/or staff must only be taken, stored and used for professional purposes in line with School policy. Images must not be distributed outside the School network/learning platform without the permission of the parent/carer, member of staff or Head teacher.
-  All use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to Line Managers or Head teacher.
-  Staff must respect copyright and intellectual property rights.
-  Staff must ensure that their online activity, both in School and outside School, will not bring their professional role into disrepute, including the use of social media sites.
-  In line with safeguarding procedures, staff must not make any comments with reference to our School, its staff, governors, pupils, families and any persons associated with it or events. Staff must not mention any information regarding activities at School, or the School in general on social networking sites.
-  Staff must report any incidents of concern regarding children's safety to the E-safety Coordinator, the Designated Child Protection Coordinator or Head teacher.
-  Staff must support the School's E-safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. Staff must be a role model and promote E-safety with students in their care and help them to develop a responsible attitude to system use, communications and publishing.
-  By signing this Staff Code of conduct, staff agree to follow the Acceptable Use policy and ICT Code of conduct and to support the safe use of ICT throughout the School.