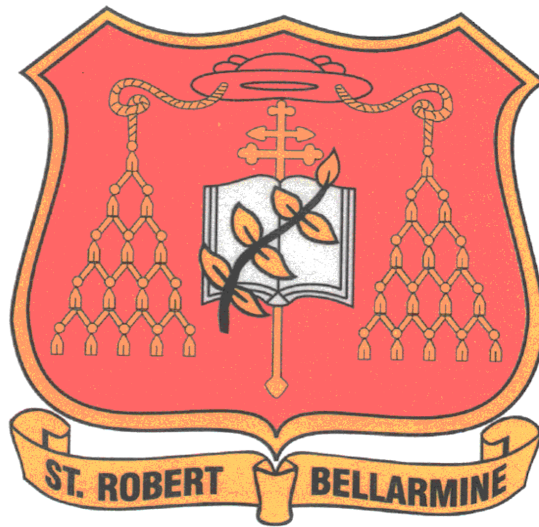


St Robert Bellarmine Catholic Primary School



Online Safety Policy

Our Mission Statement

"We are God's work of art."

- Help each other
- Be happy
- Follow the light of Jesus
- Include everybody
- Everybody do their best in every way
- Be friends with everyone
- Be responsible for your own actions
- Be Respectful
- Work to the best of your abilities
- Parents, teachers and children support each other.

Contents

1	Background information	
2	Aim	
3	Legislation	
4	Roles and responsibilities	
5	Teaching and learning	
6	Managing internet access	
7	E mail	
8	Managing filtering	
9	Password policy	
10	The school website	
11	Mobile phones	
12	Staff using work devices outside of school	
13	Social networking	
14	Cyber bullying	
15	Policy decisions	
16	Acceptable use of internet	
17	Sanctions	
18	Unacceptable use of the internet	
19	Training	
20	Protecting personal data	
21	Links to other policies	
22	Appendix 1 – Online safety training needs – self audit for staff	
23	Appendix 2 – Online safety report log	
24	Appendix 3–IT Acceptable Use Policy for Pupils Key Stage 1	

25	Appendix 4-IT Acceptable Use Policy for Pupils Key Stage 2	

1. Background information

IT in the 21st Century has an all-encompassing role within the lives of children and adults. New internet and online technologies are enhancing communication and the sharing of information. Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside of school by children and young people include:

- The Internet – World Wide Web
- e-mail
- instant messaging (often using simple web cams) e.g. Instant Messenger
- Web based voice and video calling (e.g. Skype)
- Online chat rooms
- Online discussion forums
- Social networking sites (e.g. Facebook)
- Blogs and Micro-blogs (e.g. Twitter)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Video broadcasting sites (e.g. You Tube)
- Music and video downloading (e.g. iTunes)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, messaging and internet access

2. Aim

- To have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

3. Legislation

- This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.
- It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary,

searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

- The policy also takes into account the National Curriculum computing Programmes and complies with funding agreements and articles of association.

4. Roles and Responsibilities

- **The Governing Body** has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).
- **The Headteacher** -The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- **Member of Staff/Designated Safeguarding Lead with responsibility for Online Safety** - Details of the member of staff with responsibility for Online Safety and school's Designated Safeguarding Lead (DSL) are set out in our Child Protection and Safeguarding policy and they will take lead responsibility for online safety.
- **The School IT Manager** -The school IT manager is responsible for ensuring that the schools IT systems are secure and updated and any safety incidents are dealt with in line with this policy.
- **All Staff, volunteers and visitors** - All staff, volunteers and visitors are responsible for understanding and implementing this policy.
- **Parents** - Parents are expected to ensure their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet.

5. Teaching and Learning

5.1 Why is internet use important?

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet use will enhance learning.
- The school's Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- 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 taught how to evaluate Internet content.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law as far as possible.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

6. Managing Internet Access

6.1 Information System Security

- School IT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with Sefton LA

7. Email

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- Where practicable, access in school to external personal e-mail accounts, including webmail accounts may be blocked.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

8. Managing Filtering

- The school will work with the LA and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Online Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
-

The use of filters is reviewed annually as part of the annual audit. The solution is administered and updated by a company called SENSO. Safeguarding alerts are sent direct to our Designated Safeguarding Lead and weekly monitoring reports. Any breaches are dealt with in accordance with school procedures and reported to governors. The DSL will undertake regular checks of sites that should be allowed/ blocked to check the effectiveness of the filtering solution.

9. Password Policy

- Our school makes it clear that members of our school community must always keep their password private, must not share it and must never leave it where others can find it.
- All staff have their own unique username and password to access systems – they are responsible for keeping their password private.
- We require staff to use strong/complex passwords for access to our system.
- Staff are prompted to change their password every 30 days.

10. The School Website

School values the contribution that a website can make to the life and role of the school in the modern society. A school website has five main roles:

1. To promote the school
2. To provide information to prospective parents and teachers, the wider community and the world
3. To act as a communication channel between teachers, parents, pupils and school management
4. To improve pupil learning
5. To raise standards in teaching and learning.
6. To convey messages about safety in the community

10.1 School Website Published Content

- The contact details on our website are the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Images that include pupils will be selected carefully and they will not be identified by name.
- Written permission from parents/carers is obtained before images of pupils are published electronically. This is done upon entry to school. Parents may subsequently write to agree/withdraw permission if they change their mind.

10.2 Safeguards

- The safety of pupils who appear or are referred to on the published site and extranet is of paramount importance.

10.3 Publishing names, images and work:

- Adult names will be published as their title and last name e.g. Mr. Smith
- Any images of pupils will not be labelled with their names.
- Pupils will only be shown in photos where they are suitably dressed.

- Personal details of pupils, staff and governors, such as home addresses, telephone numbers, personal e-mail addresses, etc, will not be released via the website or school e-mail.

10.4 Privacy:

- Adults have the right to refuse permission to publish their image on the published website.
- Parents have the right to refuse permission for their child's work and/or image to be published on the published website.
- Those wishing to exercise this right should express their wishes in writing to the Headteacher, clearly stating whether they object to work, images, or both being published, to the published site. Parents will be notified of this right by publication of this policy on an annual basis.

10.5 Monitoring:

- The web pages will be regularly reviewed for accuracy and will be updated as required. This review will occur at least annually. It will be the responsibility of the Site Administrator, school manager and staff to ensure this happens.

11. Mobile Phones/ Devices:

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure

- Pupils are allowed to bring their mobile phones into school for use before and after school. They MUST be signed into the school office at the beginning of the school day and signed out at the end of the school day. Any use of mobile devices in school must be in line with the school's acceptable use agreement. Any breach by a pupil may trigger disciplinary action in line with the School Behaviour policy.

- Staff are advised to use school ipads to take photos as curriculum evidence or for sharing on X (Twitter). However, if on a rare occasion they do use their own mobile, photos must be deleted once they have been uploaded and another senior member of staff confirm they have been deleted.
- Staff may use their mobile phones in school but, if it is for personal reasons, this must only happen within the staffroom when no children are present.

12. Staff Using Work Devices Outside School

- Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.
- Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.
- Any USB devices containing data relating to the school must be encrypted.
- If staff have any concerns over the security of their device, they must seek advice from the IT manager. Work devices must be used solely for work activities.

13. Social Networking

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- 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 is inappropriate for primary aged pupils.

14. Cyber-Bullying

14.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

14.2 Preventing and addressing cyber-bullying

- To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others.
- We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.
- Class teachers will discuss cyber-bullying with their children, and the issue will be addressed in assemblies.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
- The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.
- In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy.
- Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

15. Policy Decisions

15.1 Authorising Internet Access

- All staff must read and sign the 'Acceptable Use Agreement' before using any school IT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form. Upon a non-return of the form it will be assumed that the parent has granted permission for internet use.

15.2 Communication of Policy

Introducing the Online safety Policy to pupils

- Rules for Responsible Internet Use are displayed in each classroom.

- Pupils are routinely informed that network and internet use will be monitored, and a range of curriculum opportunities to gain awareness of online safety issues and how best to deal with them will be provided for pupils, as well as updates through assemblies and other forums.

Online Safety Policy and staff

- All staff will be given access to the School Online Safety Policy and its importance explained.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user.
- Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor IT use will be supervised by the DSL's and have clear procedures for reporting issues.

Enlisting support from parents

- Parents' attention will be drawn to the School's Online Safety Policy in the school prospectus and the school website.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.
- The school will publish online safety resources for parents

16. Acceptable use of the Internet

Acceptable use of the Internet is characterised when teachers ensure that the computer equipment and the Internet may only be used for legal activity consistent with the aims, objectives and rules of the school. The teacher should make sure that all users are made aware of the following rules. The guidelines will be on display in every classroom.

16.1 Conditions of Internet use

- The school and governing body have adopted conditions for Internet use, which are designed to maximise use of the Internet as a learning resource and minimise unacceptable behaviour and access to unacceptable materials.
- All users have been made aware of the conditions of use.
- Parents and carers have been made aware of the conditions of use.
- Appropriately worded copies of the Conditions of Internet Use will be displayed in every classroom, staff room and at public points of information.
- All members of staff are responsible for explaining these rules and their implications.
- All members of staff have been made aware of the possible misuses of on-line access and their responsibility towards pupils.
- The Internet policy is an integral part of the school Computing policy. All pupils, staff and other users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of Internet access rights and could lead to disciplinary action and possible criminal

prosecution. In the case of an employee breach of the conditions, this could lead to dismissal on the grounds of misconduct.

- Uses of the Internet and email facilities are intended for educational purposes only. It must be recognised that any view communicated over the Internet may be deemed to be the view of the school/governing body and in some circumstances that of the LA.
- Pupils are responsible for good behaviour on the Internet.
- Internet facilities are provided for research and communications. Parents have the right to deny access to the Internet during school time for their child. Access must be deemed a privilege rather than a right. Access requires continued demonstration of a responsible attitude and behaviour.
- Internet storage areas and other stored materials are deemed to be accessible by staff and will be reviewed to ensure responsible use.

17. Sanctions

If any breach of conditions is discovered the following sanctions may be enforced:

- Temporary or permanent ban on Internet use.
- Additional disciplinary action in line with school behaviour policies.
- Parents and other external agencies may be contacted.

18. Unacceptable use of the Internet

Unacceptable use of the Internet is not tolerated. Pupils should be aware that the following activities, whilst not an exhaustive list, are unacceptable:

1. The access to or creation, transmission or publication of any offensive, obscene or indecent images, sounds, data or other material.
2. The access to or creation, transmission or publication of any data capable of being displayed or converted to such obscene or indecent images, sounds, data or other material.
3. The creation, transmission or publication of any material, which can cause offence, inconvenience or needless anxiety.
4. The creation, transmission or publication of defamatory material.
5. The receipt or transmission of material such that this material infringes the copyright of another person or infringes the conditions of the Data Protection Act 1984.
6. Activity that threatens the integrity of the school computing systems, or activity that attacks or corrupts other systems.
7. Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received.
8. Use for personal financial gain, gambling, political purposes or advertising is forbidden.

9. Posting anonymous messages and forwarding chain letters is forbidden.
10. The transmission of unsolicited commercial or advertising materials to other users.
11. The deliberate unauthorised access to facilities, services, data or resources via the Internet.

19. Training

- All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).
- The DSL and teacher with responsibility for Online Safety, will undertake Child Protection and Safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
- Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
- Volunteers will receive appropriate training and updates, if applicable.
- More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

20. Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to GDPR compliance issued in May 2018

21. Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour for Learning Policy
- Staff Disciplinary Procedures
- Data Protection Policy and privacy notices
- Complaints Procedure

22. Appendix one – Online safety training needs – self audit for staff

Online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	Date:
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, ~~governors~~ and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

23. Appendix 2 – On line safety report log (Cpom logged)

Online safety incident report log

Online safety incident report log				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

24.Appendix 3 - IT Acceptable Use Policy for Pupils EYFS and Key Stage 1 both in school and remote learning

For Parents:

- Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should always have an entitlement to safe internet access.

This Acceptable Use Agreement is intended to ensure:

- That children will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That school 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 pupils to agree to be responsible users.

For Children:

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I will not share any personal information such as my name, age or address without a teacher's permission
- I will be polite and responsible when I send messages and communicate with others

During the school day if I am doing my school work on line I will:

- Check with a grown up before switching on
- Be ready to start my session on time
- Sit nicely just like when I am at school
- Not be eating or playing with toys during session
- Listen carefully to the adult teaching the session and remember we must take turns to speak out and not call out
- Not to press buttons to mute and unmute microphones during sessions unless I am asked to by the teacher
- End the video call when my teacher asks me to
- Tell a grown up if I see anything on screen which makes me feel worried
- Ask a grown up if I get stuck with what to click or do next
- Not share pictures or personal information with anyone other than when my teacher is talking to me

I know that if I break the rules, I might not be allowed to use a computer

Your name:

Class:

Date:

Parent / carer signature:

25. Appendix 4 - IT Acceptable Use Policy for Pupils Key Stage 2 both in school and remote learning

For Parents:

Digital technologies have become integral to the lives of children, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Children should always have an entitlement to safe internet access.

This Acceptable Use Agreement is intended to ensure:

- That children will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That school 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 pupils to agree to be responsible users.

For Children:

Acceptable Use Agreement

To keep myself safe I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I will ask permission from a teacher before using any technology devices.
- I understand that the *school* will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone will steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I will immediately report any unpleasant or inappropriate material, messages, or anything that makes me feel uncomfortable when I see it on-line.
- I will not access other people's files or send pictures of anyone without their permission.
- I understand that the *school* systems and devices are for educational use and that I will not use them for personal or recreational use unless I have permission.
- When I am using the internet to find information, I will check that the information is accurate.
- I will not use the *school* systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube).
- I will be polite and responsible when I communicate with others, I will not use inappropriate language and I understand that it is ok for others to have different opinions from me.

If I am working virtually I will:

- Check with a grown up before switching on
- Be ready to start my session on time
- Sit nicely just like when I am at school
- Not be eating or playing with toys during session
- Listen carefully to the adult teaching the session and remember we must take turns to speak out and not call out
- Not to press buttons to mute and unmute microphones during sessions unless I am asked to by the teacher
- End the video call when my teacher asks me to

- Tell a grown up if I see anything on screen which makes me feel worried
- Ask a grown up if I get stuck with what to click or do next
- Not share pictures or personal information with anyone other than when my teacher is talking to me
- I will be polite and responsible when I communicate with others, I will not use inappropriate language and I understand that it is ok for others to have different opinions from me.

I understand that if I do not follow the Acceptable Use Agreement, I may not be allowed to use any technology devices in school and my parents/carers may be contacted.

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

- I use the school systems and devices and own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website etc.

Your name:

Class:

Date:

Parent / carer signature: