St.Mary's Catholic Primary School

Part of The Christus Catholic Trust

Internet Safety Policy

Respect Ourselves, Respect Others, Respect our School, Love God

This school is committed to safe guarding and promoting the welfare of children and young people and expects all staff and volunteers to share in this commitment

Internet Safety Policy

Our Mission Statement

Respect Ourselves, Respect Others, Respect our School, Love God

Teaching and Learning

1. Why is use of the Internet so 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 safety is taught throughout the planning in each class and we explicitly teach internet safety through the internet safety week in February each year.

2. What are the benefits of using the Internet for the education of our children?

2.1 Access to world-wide educational resources including museums and art galleries;
2.2 Educational and cultural exchanges between pupils world-wide;
2.3 Access to experts in many fields for pupils and staff;
2.4 Staff professional development through access to national developments, educational materials and good curriculum practice;
2.5 Communication with support services, professional organisations and colleagues;
2.6 Improved access to technical support including remote management of networks and exchange of curriculum and administrative data at both local and national government levels.

3. How will Internet use enhance the learning of pupils?

3.1 The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
3.2 Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
3.3 Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

4. How will pupils be taught to evaluate Internet content?

4.1 The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
4.2 Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
4.3 Pupils will be taught how report any inappropriate material or messages to CEOP.

Managing Internet Access

5. Information system security

5.1 School ICT systems capacity and security will be reviewed randomly throughout each year.
5.2 Virus protection will be updated regularly.

5.3 Security strategies will be discussed with the local authority.

6. E-mail

6.1 Pupils may only use approved e-mail accounts on the school system.

6.2 Pupils must immediately tell a teacher if they receive offensive e-mail.

6.3 Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

6.4 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.

6.5 The forwarding of chain e-mails or letters is not permitted nor is potentially offensive communications.

6.6 Access by pupils to external personal e-mail accounts whilst in school will not be permitted.

7. Published content and the school web site

7.1 The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

7.2 The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

8. Publishing pupil's images and work (including video)

8.1 Images taken for the purpose of recording a child or group of children participating in activities or celebrating their achievements is an effective form or recording their progression. However, it is essential that images are taken and stored appropriately to safeguard the children in our care.

8.2 No images electronically or printed are to be taken home.

8.3 Only the designated cameras are to be used to take any images within the setting or on outings. Images taken on this camera must be deemed suitable without putting the child/children in any compromising positions that could cause embarrassment or distress. All staff are responsible for the location of the cameras; they should be placed in a safe place at the end of every day. Images taken and stored on the camera must be downloaded as soon as possible, ideally once a week.

8.4 Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with images.

8.5 Written permission from parents or carers will be obtained before images of pupils are published on the school Web site.

8.6 Pupil's work can only be published with the permission of the pupil and parents.

8.7 Under no circumstances must cameras of any kind (including mobile phones) be taken into the children's toilets or changing rooms or any other place which could be considered as unsafe in child protection terms.

8.8 Failure to adhere to the contents of this policy will lead to disciplinary procedures being followed.

9. Social networking and personal publishing

9.1 The school will block/filter access to social networking sites.

9.2 Newsgroups will be blocked unless a specific use is approved.

9.3 Pupils will be advised never to give out personal details of any kind which may identify them or their location.

9.4 Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

9.5 Should it come to the school attention that a child is using a social networking site the school will discuss with the parents to advise against its use.

9.6 However if a child is offensive on a social networking site we will report it to the site to deal with as appropriate.

10. Managing filtering

10.1 The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

10.2 If staff or pupils discover an unsuitable site, it must be reported to the Internet Service Provider via the ICT Co-ordinator or head teacher.

10.3 Staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

10.4 The internet settings also hold another layer of filtering settings by using the Proxy Server Port number 8082.

11. Managing videoconferencing

11.1 Pupils should ask permission from the supervising teacher before making or a conference call.

11.2 Videoconferencing will be appropriately supervised for the pupils' age.

12. Managing emerging technologies

12.1 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

12.2 Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

13. Protecting personal data

13.1 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

14. Authorising Internet access

14.1 All staff must read and sign the 'staff information systems code of conduct' before using any school ICT resource.

14.2 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.

14.3 At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

14.4 Parents will be asked to sign and return a consent form.

15. Assessing risks

15.1 In common with other media such as magazines, books, videos and DVDs, some material available via the Internet is unsuitable for our 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. Neither the school nor Thurrock Local Authority can accept liability for the material accessed, or any consequences of Internet access.

15.2 The school will audit ICT provision to establish if the internet safety policy is adequate and that its implementation is effective.

16. Handling internet safety complaints

16.1 Complaints of Internet misuse will be dealt with by a senior member of staff.

16.2 Any complaint about staff misuse must be referred to the headteacher.

16.3 1Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Communications Policy

17. Introducing the internet safety policy to pupils

17.1 Internet safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.

17.2 Pupils will be informed that network and Internet use will be monitored.

18. Staff and the internet safety policy

18.1 All staff will be given the School internet safety Policy and its importance explained.

18.2 Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

19. Enlisting parents' support

19.1 Parents' attention will be drawn to the School internet safety Policy in newsletters, the school brochure and on the school Web site.

Staff Guidelines for the use of social networking sites

20. General Practice and Advice

- At no time must any photographs or materials be published on a social networking site that identify St Mary's Catholic Primary School. Photographs of staff at work may only be used with the express permission of the staff members concerned.
- Any member of staff found to be posting remarks or comments that breach confidentiality and/or are deemed to be of a detrimental nature to the reputation of the school or other employees will face disciplinary action in line with the school's disciplinary procedures.
- Any member of staff found to be posting/publishing photographs of the setting, children or staff unless staff permission has been gained will face disciplinary action in line with the school's disciplinary procedures.
- Members of staff should not be in contact with current St. Mary's Catholic Primary School pupils via social networking sites such as Facebook.com and others, in accordance with the School's Safeguarding and Welfare policy.
- Members of staff with Facebook profiles should set the privacy levels on their accounts to maximum i.e. only people on their friend's list should be able to view their pictures/private information. This can be done by going to Setting > Profile and adjusting the parameters accordingly.

- Members of staff with distinctive surnames should be aware that it will be relatively easy for pupils to track them down on Facebook i.e. due to the large number of people named John Smith it is difficult to trace a specific individual.
- Members of staff should note that although these measures will make it harder for pupils to find them on a social networking site determined individual with knowledge of how the website works will eventually be able to trace a person down (given enough time).

21. Action to be taken if a member of staff is contacted by a pupil

There are two types of contact through Facebook:

1. A message
2. An invitation to be added to a person's "Friends list" If a message from a pupil is received the following action should be taken:
   a) Do not reply to the message
   b) A senior member of staff should be contacted at the earliest opportunity and informed
   c) The pupil should be reminded of the School's internet safety policy.

If an invitation to a person's friends list is received the following action should be taken:

a) Immediately reject the invitation
b) Senior Staff should then be asked to speak to the pupil on behalf of the member of staff who was contacted.
c) The pupil should be reminded of the School's internet safety Policy.

St Mary's Catholic Primary School
Staff Information Systems Code of Conduct

Academic Year 2020/2021

To ensure that staff are fully aware of their professional responsibilities when using information systems (computers, cameras, phones, and any other devices), they are asked to sign this code of conduct. Staff should consult the school's internet safety policy for further information and clarification.

- The information systems (including computers, cameras, and any other computing equipment bought by the school) are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems (including computers, cameras, and any other computing equipment bought by the school) use will always be compatible with my professional role.
- I understand that school information systems (including computers, cameras, and any other computing equipment bought by the school) may only be used for school use.
- I understand that the school may monitor my information systems (including computers, cameras, and any other computing equipment bought by the school) and Internet use to ensure policy compliance randomly and throughout each school year.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school internet safety Coordinator and the Designated Child Protection Coordinator.
- I will not post on any social media or in any public domain, remarks or comments that breach confidentiality and/or are deemed to be of a detrimental nature to the reputation of the school, children, parents, governors and staff. I understand that I will face disciplinary action in line with the school's disciplinary procedures if I do so.
- I will not share information relating to pupils, staff, governors and parents to anyone who is not employed at the school.
- I will promote internet safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- Use of any school mobile phone must be used in accordance with my professional role.

NB: Personal mobile phones, tablets, any recording or computing device are not allowed to be used in school, on residential trips or for any school related matters. Any failure to comply with this will result in disciplinary action being taken.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: _____ Name:_____

Dated:

Policy Name: **Internet Safety**		
Reviewer: M Jones	Reviewed Date: December 2020	Date of next review: September 2021