# St Catherine's Catholic Primary School

## E-SAFETY POLICY

Policy Date: November 2017

Review Date: November 2018

## Contents

## 1. Overview

1.1 We are committed to using Information and Communication Technology and all it offers to promote learning in the most effective and appropriate way at our School - for the benefit of our pupils, staff and community. To this end, we have developed this Acceptable Use Policy, to provide safeguards and ensure that all members of our School community understand the benefits, risks and what is expected of them when they use ICT in the learning environment.

1.2 Our policy consists of:

- Statements outlining our School's approach and attitudes towards using Information & Communications Technologies safely and responsibly
- Clear guidelines and rules for acceptable use of ICT.
- There are also Internet Use Agreements, to be signed by parents, staff and pupils

1.3 The E-Safety Policy will operate in conjunction with other policies including those for ICT, behaviour, bullying, curriculum, child protection, data protection and security. The School's ICT subject leader will also act as the e-safety coordinator. The e-Safety Policy and its implementation will be reviewed regularly to ensure that it remains fit for purpose.

## 2. Why Internet Use is Important

2.1 We believe the internet is an essential element in the 21st century life for education, business and social interaction.

2.2 The School recognises its duty to provide children with quality Internet access as part of their learning experience.

2.3 Using the internet and ICT in general is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.4 Pupils are increasingly using the internet and a range of ICT devices outside of School life and therefore need to learn how to evaluate information and to take care of their own safety and security.

## 3. Using the Internet for Learning in Academies

3.1 We teach all of our pupils how to find appropriate information on the internet and how to ensure as far as possible, that they understand who has made this information available and how accurate and truthful it is.

3.2 Teachers carefully plan all internet-based teaching and lessons to ensure that pupils are focused and using appropriate and relevant materials.

3.3 Children are taught how to use search engines and how to evaluate internet-based information as part of the ICT curriculum, and in other curriculum areas where necessary.

3.4 Pupils are taught what internet use is acceptable and what is not and given clear objectives for internet use.

3.5 Pupils are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

3.6 Pupils in Key Stage 1 will not be permitted to 'free-surf' the web. In Key Stage 1 and typically in Key Stage 2, pupils' internet access will be through a selection of evaluated sites suitable for the purposes of the task.

3.7 Processes are in place for dealing with any unsuitable material that is found during internet use (see section on managing filtering).

3.8 Where pupils are allowed to freely search the internet, e.g. using search engines, staff are vigilant in monitoring the content of the websites the young people visit. Pupils who need to search individually will be in the upper primary years. Teachers, wherever possible, will have viewed the content prior to use to check its relevance and suitability.

3.9 The School's internet access includes filtering appropriate to the age of our pupils which is provided by an approved supplier.

3.10 The School enables the pupils to access the internet at lunchtime as part of a range of activities for young people. There are clear guidelines (see appendix 1) as to what is accessed and it is monitored by the SLT on duty at lunchtime, regulated in access by the teaching staff and supported by specialist ICT support staff.

## 4. Evaluating Internet Content

4.1 The School will ensure that staff and pupils are mindful of copyright regulations when copying, downloading and representing materials from the internet. Web-based resources have similar copyright status to printed and recorded materials, such as books, films and music, and this must be taken into consideration when using them.

4.2 Pupils, during Key Stage 2, will 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 to carry out simple checks for bias and misinformation.

4.4 Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

## 5. Internet Use by Staff

5.1 Our School understands that the internet is a valuable resource for School staff. It provides a wealth of resources, teaching materials and information that we can use to support and enhance learning. It allows staff to share resources with other academies, and to engage in debate and discussion on educational topics and news.

5.2 It also provides an efficient way to access information from the Department for Education and other government agencies and departments that will help staff to keep abreast of national and local developments.

5.3 There are also increasing opportunities for staff to access INSET and Continuing Professional Development activities using the Internet and e-learning resources.

5.4 We are committed to encouraging and supporting our School staff to make the best use of ICT and all the opportunities it offers to enhance our teaching and support learning.

5.5 Staff use of the internet on School computers will be responsible and legal at all times and in keeping with their professional role and responsibility. Misuse of the internet and School computer systems will be rigorously investigated.

## 6. E-mail

6.1 E-mail is one of the many modes of communication which plays an important role in many aspects of our lives today. We teach the use of e-mail as part of our ICT curriculum by means of safe sites such as www.epals.com. This is a secure means of children communicating with children in other academies. Open email contact is not possible. This provides a limited facility and yet it gives all the structure of using actual email.

6.2 In spite of this not being an open facility the opportunity is taken to educate children to be aware of the benefits and risks and how to be safe and responsible users as part of our e-safety provision.

6.3 Pupils are taught strategies to deal with inappropriate emails and are reminded of the need to write emails clearly and correctly, not including any unsuitable or abusive material.

6.4 Pupils are taught not to reveal personal details of themselves or others in e-mail communication, nor to arrange to meet anyone without specific permission.

6.5 Staff are encouraged to use the School email service and accounts that are available. They are more secure and are easier to access by a third party should the need for scrutiny arise. Personal web based email accounts are also permitted but discouraged for professional communications.

6.6 Staff should always ensure that they represent the School in a professional and appropriate way when sending e-mail, contributing to online discussions or posting to public websites. Failure to do so could lead to disciplinary action being taken.

## 7. Published Content and the School Website

7.1 The contact details on the School web site will be the School address, e-mail and telephone number.

7.2 Individual personal contact information will not be published.

7.3 The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. It will be the responsibility of other staff, personally or by delegation to update the website regularly.

7.4 The School maintains a separate website policy and has a clear policy attached to its website.

## 8. Publishing Pupils' Images and Work

8.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images and video that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images / video on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

8.2 The School will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

8.3 Staff are allowed to take digital / video images to support educational aims, but must follow the School policy concerning the sharing, distribution and publication of those images which states that:

- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute or danger;
- Nobody should take, use, share, publish or distribute images of others without their permission;
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images;
- Pupils' full names will not be used anywhere on the website or learning platform, particularly in association with photographs;
- Parents or carers are informed of our policy on publishing and are able to opt their children out.

## 9. Communication Technologies – Including Chat, Forums, Blogs, Instant Messenger Services, Social Networking Sites

9.1 Most of these modes of electronic communication are restricted in the School however they are being used more frequently by pupils and staff outside of the School.

9.2 We acknowledge social networking sites, blogs, instant messenger services, chat rooms and forums are beneficial for communication, learning and research. They also present a range of personal safety and privacy issues.

9.3 In School time, pupils and staff are not permitted to access social networking sites, public chat rooms, discussion groups and forums etc. using School resources. Most are blocked by the filtering service used by the School.

## 10. Mobile Phones and Other Handheld Devices (Including Those that are Internet Enabled)

10.1 We anticipate that more and more of our pupils will have access to internet-enabled devices such as mobile phones or other hand held devices which are capable of browsing and uploading to the internet, accessing email and social networking services, as well as taking photos and recording video.

10.2 The School recognises the potential advantages these devices can offer for staff and pupils and there are clear and enforceable rules for their use.

10.3 Pupils are taught the legal and moral implications of posting photos and personal information from mobile phones to public websites and how to use these technologies in a safe and responsible manner.

10.4 Children must not bring mobile phones to the School. Only in exceptional, prior arranged circumstances will the School permit mobile phones belonging to pupils on the School premises during School sessions. If such a set of circumstances is deemed necessary, the mobile phone will be kept securely by the pupil's class teacher.

10.5 Staff should represent the School in a professional and appropriate way when communicating via the internet, contributing to online discussions or posting to public websites using School facilities.

## 11. Electronic Communications with Children by Staff

11.1 Communication between children and School staff should take place within clear and explicit professional boundaries.

11.2 Staff must be careful not to share any personal information with children such as email, web based communication facilities, home or mobile numbers. They should not request, or respond to, any personal information from the child / young person, other than that which might be appropriate as part of their professional role.

11.3 Staff should ensure that all communications are transparent and open to scrutiny. In addition all staff must be sure of their social networking and uphold professional confidentiality at all times. As a staff we have agreed that we should not accept parents or pupils as 'friends' on social contact sites such as Facebook.

## 12. Downloads

12.1 The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of School equipment.

12.2 Pupils are not allowed to download any material from the internet unless directed to do so by an appropriate staff member.

12.3 Staff should take care that files from both other computers outside the School and internet are checked for virus contamination before they are used on the School system.

12.4 Pupils are not allowed to use CDs, DVDs or memory sticks brought from home or, for example, from magazines unless they have been given permission.

12.5 The School subscribes to suitable antivirus software. The software is updated regularly and virus detection is monitored by the School's technician.

## 13. Managing Filtering

13.1 Whilst filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken.

13.2 The action will include:

1. Making a note of the website and any other websites linked to it;
2. Informing the ICT leader and Headteacher;
3. Logging the incident;
4. Informing the Internet Service Provider so that the website can be added to the content filter if appropriate;
5. Discussion with the pupil about the incident, and how they might avoid similar experiences in future
6. Parents will be informed where necessary.

13.3 The School will work with the local authority, CLEOPS and our Internet Service Provider to ensure systems to protect pupils and staff are effective and appropriate.

13.4 Pupils or staff who deliberately try and access unsuitable materials will be dealt with in accordance with the School's discipline policies for pupils and staff.

## 14. Managing Emerging Technologies, Video-Conferencing and Electronic Resources for Learning

14.1 Emerging technologies and resources will be examined for educational benefit and a risk assessment will be carried out before use in the School is permitted.

## 15. Online Bullying and Harassment (Cyberbullying)

15.1 Online bullying and harassment via Instant messaging, chat rooms, social networking sites etc. are potential problems that can have an effect on the well being of pupils and staff alike.

15.2 Our School has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy. These include:

- No access in the School to public chat-rooms, instant messaging services and social networking sites;
- Pupils are taught how to use the internet safely and responsibly which includes how to identify and respond to 'cyberbullying';
- Children are taught how and where to report incidents that make them feel unhappy or worried;
- As with any form of bullying, we encourage pupils to discuss with staff any concerns or worries they have about online bullying and harassment.

## 16. Authorising Internet Access

16.1 All staff must read and sign the 'Acceptable ICT Use Agreement' before using any School ICT resource.

16.2 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.

16.3 At Key Stage 1, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials. Parents are asked to sign and return a consent form when their child starts at the School.

## 17. Assessing Risks

17.1 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.

17.2 The School can't accept liability for the material accessed, or any consequences of Internet access.

17.3 The School will audit ICT provision to establish if the E-safety policy is adequate and that its implementation is effective.

## 18. Handling E-Safety Complaints

18.1 Online safety incidence reporting log-book to be kept centrally in the school office.

18.2 Any complaint about staff misuse must be referred to the Headteacher (See Appendix 1)

18.3 Complaints of a child protection nature must be dealt with in accordance with the School child protection procedures.

18.4 Pupils and parents will be informed of the complaints procedure.

## 19. Introducing the E-Safety Policy to Pupils

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

19.2 Pupils will be informed that network and Internet use can be monitored.

19.2 Pupils to be made aware of Acceptable Use Policy and all children transitioning into KS2 to read and sign Acceptable Use Policy for older users.

## 20. Staff and the E-Safety policy

20.1 All staff will be given access to the School E-Safety Policy and its importance will be explained. A programme of E-safety training will be available to staff who can also discuss matters with the E-Safety Coordinator on an ad-hoc basis.

20.2 Staff should be aware that internet traffic can be monitored and traced to the individual user.

20.3 Discretion and professional conduct is essential.

20.4 All new staff should receive E-safety training as part of their induction programme, ensuring that they fully understand the School Acceptable Use Policy

20.5 The E-Safety Coordinator will receive regular updates through attendance at training sessions and / or by reviewing guidance documents released by appropriate authorities and providers.

## 21. Enlisting Parental Support

21.1 Some parents and carers might have a limited understanding of E-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of children's on-line experiences.

21.2 Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

21.3 The School provides information and awareness to parents and carers through:

- Information in School newsletters;
- Links to resources from the School website;
- Parent workshops.
- School welcome pack.

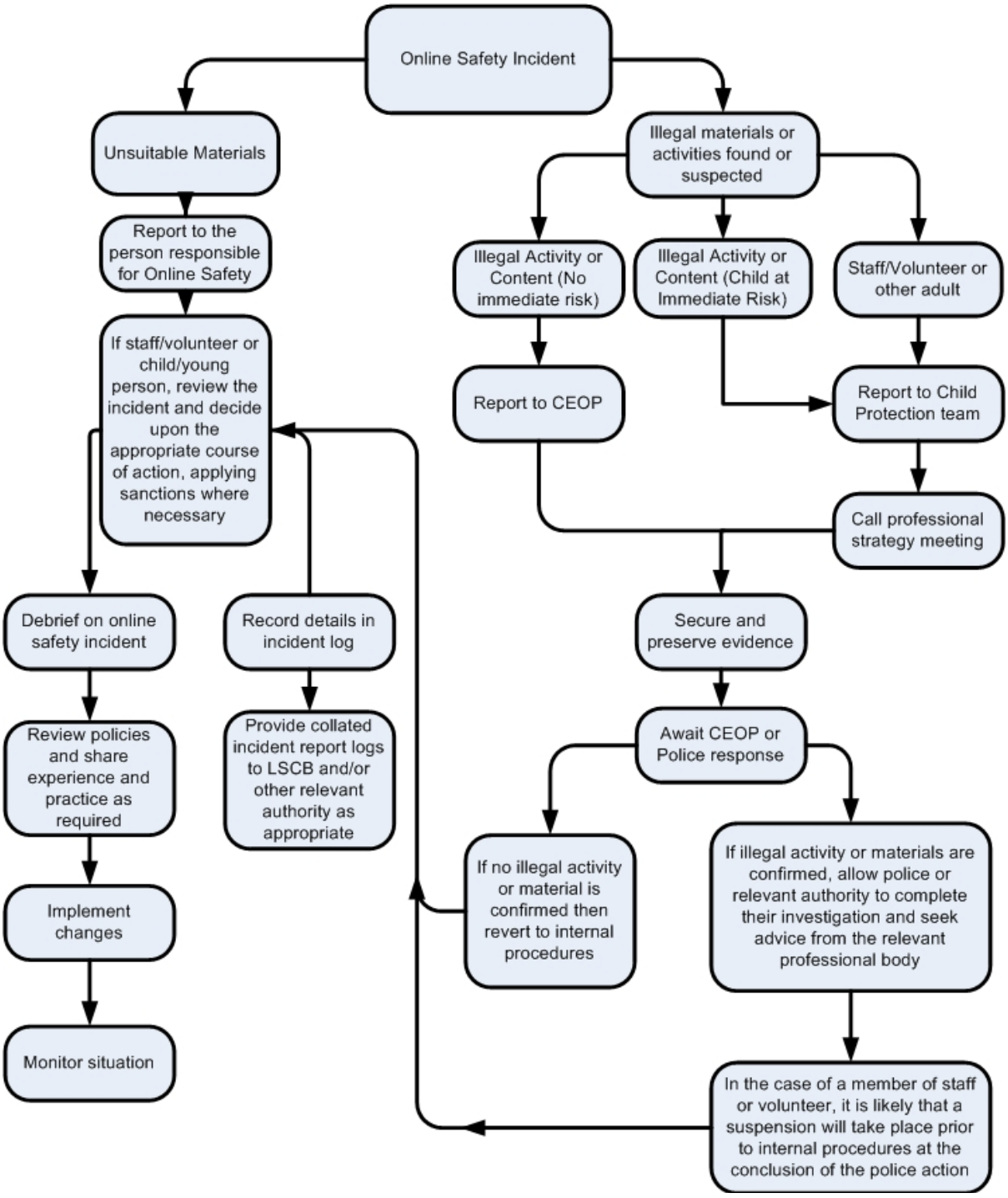
## 22. Governors

22.1 Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in ICT / E-safety/ health and safety / child protection.

22.2 This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governor Association or other relevant organisation;
- Participation in School training / information sessions for staff or parents.

**(Appendix 1) Responding to incidents of misuse – flow chart**



**Record of reviewing devices / internet sites (responding to incidents of misuse)**

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

.....

### *Details of first reviewing person*

Name: .....

Position: .....

Signature: .....

### *Details of second reviewing person*

Name: .....

Position: .....

Signature: .....

### Name and location of computer used for review (for web sites)

.....

.....

| *Web site(s) address / device* | *Reason for concern* |
|---|---|
| | |
| | |
| | |
| | |
| | |

### *Conclusion and Action proposed or taken*

| | |
|---|---|
| | |
| | |
| | |
| | |
| | |