Holy Trinity Catholic Primary School E-safety Policy

1. Who will write and review the policy?

The school has a designated ICT coordinator and DSL.

Our e-safety Policy has been written by the school, building on government guidance. The policy has been agreed by the leadership team and approved by the Governing Body. It will be reviewed regularly. Changes will be made immediately if technological or other developments so require.

2. What is e-Safety?

E-Safety encompasses Internet technologies and electronic communications such as mobile phones. This policy highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experiences.

The previous policy; ‘Internet Access Policy’, has been revised and renamed as the school’s e-safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

This policy will operate in conjunction with other school policies including those for Computing, behaviour, bullying, PSHCE and child protection.

TEACHING & LEARNING

3. Why is Internet use important?

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

Internet use is a necessary tool for learning.

Internet access is an entitlement for students who show a responsible and mature approach to its use.

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. Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

4 How does the Internet benefit education?

Benefits of using the Internet in education include:

Access to world-wide educational resources including museums and art galleries;

Educational and cultural exchanges between pupils world-wide;

Cultural, vocational, social and leisure use in libraries, clubs and at home;

Access to experts in many fields for pupils and staff;

Professional development for staff through access to national developments, educational materials and effective curriculum practice;

Collaboration across support services, professional associations and between colleagues;

Improved access to technical support including remote management of networks and automatic system updates;

Access to tools of direct communication, including video conferencing and email;

Exchange of curriculum and administration data with BDES, OCC and DFE; and

Access to learning whenever and wherever convenient

5 How can Internet use enhance learning?

The school 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.

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils’ age and maturity.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

6 How will pupils learn to evaluate Internet content?

If staff or pupils discover unsuitable sites the URL (address) and content must be reported to the Internet Service Provider via the Computing subject leader/System Administrators. Pupils must follow the procedure for reporting unsuitable Internet content which is shared with all pupils by their class teacher.

The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. E.g Wikipedia

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

The evaluation of on-line materials is a part of every subject.

MANAGING INFORMATION SERVICES

7. How will our ICT system security be maintained?

The school ICT systems will be reviewed regularly with regard to security.

Virus protection will be installed and updated regularly.

Use of data storage facilities (mobile storage) by pupils within school is prohibited to protect against virus transfer.

Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.

The Computing Subject Leader and Network Manager will review periodically that the system has the capacity to take increased traffic caused by Internet use.

The use of user logins and passwords to access any school subscription services will be enforced. Pupils and their parents will be reminded of the importance of keeping such details secure and not sharing with their peers or other adults.

8. How should Web site content be managed?

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

The Headteacher will take overall editorial responsibility and ensure content is accurate and appropriate on all pages directly related to the day-to-day workings of the school.

The Website should comply with the school's guidelines for publications.

The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

9. Can pupils' images or work be published?

Images which include pupils will be selected carefully and only those children whose written parental permission has been sought will be identifiable.

Written permission is given by parents when children join. This data is held on the school's SIMS network.

Pupils' full names will not be used on the Website when associated with photographs, or in any way which may be to the detriment of pupils.

Pupil photographs will immediately be removed from the school Website upon request from parents, or other appropriate request.

10. How will social networking and personal publishing be managed?

The school will block access to social networking sites.

Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.

Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.

Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

Students should be advised not to publish specific and detailed private thoughts.

Teachers should be advised not to run social network spaces for student use on a personal basis.

11. How will filtering be managed?

The school will work in partnership with parents, 123ICT and the Internet Service Provider to endeavour that systems to protect pupils are reviewed and improved.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Computing Subject Leader/ Designated e-Safety Coordinator who will liaise with 123ICT to plan action to be taken.

Any material that the school believes is illegal must be referred to the co-ordinator or CEOP (please see references given later).

12. How will video conferencing be managed?

Currently not applicable

13. How can emerging Internet uses be managed?

Emerging technologies will be examined for educational benefit before use in school is allowed by Computing subject leader and senior management team.

Mobile phones will not be used by pupils during lessons or on the school premises at any time of the day.

The school should investigate wireless, infra-red and Bluetooth communication technologies and decide a policy on phone use in school as new technologies become available. Computing subject leader will present findings to senior management team and amend the relevant policies as required.

14. How should personal data be protected?

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

POLICY DECISIONS

15. How will Internet access be authorised?

All staff and pupils will initially be granted access to the school's electronic communications.

Parents will be informed that pupils will be provided with supervised Internet access.

Parents will be asked to sign and return a consent form when they join St. Mary's Catholic Primary School

Pupils will not be allowed to use computers or Ipads with Internet unless there is a responsible adult present to monitor its usage. We rely upon the filtering system deployed to block inappropriate content and adults are present to advise pupils if they discover information that they do not understand or need to verify the content of web pages.

16. How will the risks be assessed?

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and linked nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

The Headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

17. How will e-safety complaints be handled?

Complaints about Internet misuse will be dealt with under the School's complaints procedure. Any complaint about staff misuse must be referred to the Headteacher.

Pupils and parents will be informed of the complaints procedure.

Parents and pupils will need to work in partnership with staff to resolve issues.

There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

Sanctions available include: - interview/counselling by senior member of staff/class teacher/teaching assistants; - informing parents or carers; - removal of Internet or computer access for a period, which could prevent access to school work held on the system.

18. How is the Internet used across the community?

The school will liaise with local organisations to establish a common approach to e-safety.

The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

19. How will Cyberbullying be managed?

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF2007. Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety. There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying.

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

All incidents of cyberbullying reported to the school will be recorded.

There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.

Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.

20. The use of mobile phones

The use of phones and other personal devices by staff in school will be decided by the school. The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.

- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Pupils must not use phones or electronic devices brought from home under any circumstances while on the school site. They are to be handed into the school office as soon as children enter the building in the morning and children collect them again at the end of the day.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will be issued with use of a school phone where contact with pupils or parents/carers is required.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.

- If a member of staff breaches the school policy then disciplinary action may be taken.

COMMUNICATIONS POLICY

21. How will the policy be introduced to pupils?

Rules for Internet access will be discussed with pupils on a regular basis.

An e-safety training programme will be introduced to raise the awareness and importance of safe and responsible Internet use both at school and home.

Internet safety guidelines will be prominently linked from the home page of the school's intranet and Internet sites.

Pupils will be informed that Internet use will be monitored.

Pupils receive e-safety lessons regularly, as do staff and parents. A specific module of work focusing on E-safety is taught in every year group annually.

Instruction in responsible and safe use should precede Internet access.

22. How will the policy be discussed with staff?

All staff will be given access to the School e-Safety Policy and its application and importance explained.

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

The monitoring of Internet use is a sensitive matter. Staff should only operate monitoring procedures on instruction from the Leadership Team.

23. How will parents' support be enlisted?

Parents' attention will be drawn to the School e-Safety Policy via the school prospectus and on the school website.

Internet issues will be handled sensitively to inform parents without undue alarm.

A partnership approach with parents will be encouraged. This will include leaflet distributions, demonstrations, practical sessions and suggestions for safe Internet use at home.

Training for parents will be held on a two yearly basis or where specific need arises.