St Chad's Catholic Primary School
E-Safety Policy

School Mission Statement:

"At St Chad's we grow in the light of Christ, to share his love and reflect the gospel values"

1. Introduction

1.1 The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to e-safety.

1.2 Young people have access to the Internet from many places; home, school, friend's homes, libraries and in many cases mobile devices. Our school has a number of services to help ensure that curriculum use is safe and appropriate, however access out of school does not usually have these services and has a range of risks associated with its use. Schools are ideally placed to help young people learn to become e-safe whilst in school and at home.

2. Internet

2.1 The purpose of Internet access at St Chad's School is to support and develop educational standards, support the professional work of the staff and to enhance the school's management information and administration systems.

2.2 Access to the Internet is a necessary tool for staff and students. It helps prepare children for the future and personal development needs. It is a requirement of the National Curriculum for Computing and is implemented across the curriculum.

2.3 Internet access is provided and filtered by the Birmingham Grid for Learning (BGFL) and is designed for pupils and staff. BGFL has strong filtering systems in place that are age and content appropriate for pupils.

2.4 Internet access is planned to support, develop and extend learning activities.

2.5 Access levels are reviewed to reflect the current curriculum.

2.6 Staff will select sites which support the learning outcomes planned for the pupils' age and maturity.

2.7 Pupils are given clear objectives for Internet use and sign an Internet agreement.

2.8 Pupils are taught how to take responsibility for their own Internet access during lessons.

3. Email

3.1 Pupils may only use the approved email accounts given to them on the school system. Children are not allowed to access personal email accounts or chat rooms whilst in school.

4. Information System Security

4.1 The security of the schools information systems will be reviewed regularly.
4.2 Virus protection will be installed and updated regularly.
4.3 The school uses broadband with firewall and filters.

5. School Website

5.1 The Computing coordinator, Headteacher and Deputy Headteacher will take overall editorial responsibility for content on the school website and ensure it is accurate and appropriate

6. Publishing pupils images and work

6.1 Parents will be given the opportunity annually, to inform the school if they do not want their child/ren's photographs to be published on the school's website.
6.2 Pupil's full names will not be displayed anywhere on the school website.
6.3 Pupil's work will only be published with the permission of the pupil and parents.

7. Social Networking and Personal Publishing

7.1 Social networking sites will be blocked unless a specific use is approved.
7.2 Pupils are advised never to give out personal details of any kind which may identify them or their location.
7.3 Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils

8. Managing Filtering

8.1 The school works in partnership with the service provider and BGFL to ensure filtering systems are as effective as possible.
8.2 If staff or pupils discover unsuitable sites, the school Forensic software will automatically capture a screen shot of that site and it will be automatically sent to the Head Teacher where they will determine action required.

9. Emerging Technologies

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

10. Authorising internet access

10.1 The school will keep an up to date record of all staff and pupils who are granted Internet access.
10.2 All staff must read and sign the ICT Acceptable Use Policy.
10.3 Parents and pupils will be asked to sign and return a consent form agreeing to comply with the schools Acceptable Use Policy.

11. Assessing Risks

11.1 The school will take all reasonable precautions to ensure that users only access appropriate material. However, due to the world wide scale and linked nature of the Internet, it is not possible to guarantee that unsuitable material will never appear on a school iPad or computer. The school cannot accept any liability for the material accessed, or any consequences of Internet access.

11.2 The Headteacher, Deputy Headteacher and the Computing coordinator will ensure the E-safety Policy is implemented and compliance with the policy is monitored.

12. E-Safety Complaints

12.1 Any E-safety issues or complaints must be reported to the ICT Coordinator. These will then be passed on the Headteacher or Deputy Headteacher.

12.2 Any complaint of a child protection nature must be dealt with in accordance to the school's child protection procedures.

13. Communication of the E-Safety Policy

13.1 Rules for Internet access will be displayed in each classroom.

13.2 Pupil will be informed that Internet use will be monitored.

13.3 Advice on E-Safety will be introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use.

13.4 All staff will be given the E-Safety policy and its importance explained.

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

Policy Written: July 2014

Policy to be reviewed: Autumn 2015

Signed:

Date: