

## College Road Primary School E- Safety Policy



College Road  
Primary School

### **What is included?**

The school will ensure that all members of the school community are aware of the E-safety policy and the implications for the individual. E-safety depends on staff, governors, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies.

This e-safety policy considers the use of both the fixed and mobile internet, PCs, laptops, webcams, digital video equipment, mobile phones, camera phones, personal digital assistants and portable media players. It will however be revised to incorporate new and emerging technologies.

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

By the end of Autumn Term 1, in each new academic school year, **all** pupils will have participated in a 'Cyber Safety' lesson. The principles of this will be threaded throughout the ICT curriculum when appropriate.

### **Use of the Internet**

The Internet is now considered to be an essential part of modern life. In addition, the school has a duty to provide pupils with quality Internet access as part of their learning.

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 information systems. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for students who show a responsible and mature approach to its use. However all pupils and staff must sign a responsible use of the internet form prior to using the school internet.

Use of the internet is monitored by Light Speed Web Filter Access and logs are checked by an adult weekly. In addition to this teachers have a responsibility to check web sites before recommending them to children. Furthermore pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Where Internet activities are part of the curriculum they will be planned so that they enrich and extend the learning activities. Staff will guide pupils through on-line activities that will support the learning outcomes planned for the age and maturity of the pupils. All websites used for specific activities will have been approved by the person providing the lesson. Although staff may wish to find and recommend further websites, there is a list of suggested websites on the school server.

Curriculum activities that involve the use of the Internet for gathering information and resources independently will help develop pupil skills in locating and evaluating material at home and in school. Subsequently this can sometimes lead to children accidentally viewing a site they shouldn't. As a school we have Internet access that is

monitored by Light Speed Web Filter Access and logs are checked by an adult weekly to help avoid this, but parents may wish to consider their own monitoring programme.

However, should a site be accessed that is deemed unsuitable, or inappropriate content is encountered, staff and pupils should follow the school procedures for such events:

- Pupils must report unsuitable material, to a teacher. The teacher will then ensure that the reporting procedures are followed.
- Unsuitable URL addresses will be reported through the headteacher who will report it to our paid ICT technical support.
- Parents will be informed of such incidents sensitively to avoid undue distress.

In addition to this, school will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.

### **Email**

Curriculum activities that involve the use of e-mail will be delivered through email programmes that are controlled by the school and only use email accounts that are approved by the school.

Pupils will never reveal personal details of any member of the school community in E-mail communications.

Pupils have email accounts that can be used to message each other internally. The use of individual pupil personal accounts will not be permitted through the school system.

Any e-mail sent to an external account will be authorised by the school, before sending, following the same procedure used for letters written on school headed notepaper.

Any email received that is deemed to be inappropriate should be reported to the headteacher at once.

The forwarding of chain letters is not permitted.

### **Social Networking**

The use of online chat rooms, instant messaging services and text messaging will not be allowed until the school community agrees that these technologies can be supervised or monitored in a way that will guarantee the e-safety of the pupils. Thus social networking sites and newsgroups will be blocked and filtered.

Pupils are advised never to give out any personal details that might identify them or their location.

Pupils are advised not to place personal photos on any social network space.

Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals.

Pupils are advised never to agree to meet someone they have met on a social networking site.

Should pupils have any concerns about social networking sites or chat rooms, they are advised that they must tell an adult.

### **Mobile Phones**

The use of mobile phones will not be permitted during lessons or formal school time by staff or pupils. This excludes occasions when staff may need to use mobile phones, for example on school trips, or as part of a demonstration in a lesson. This is to avoid the possibility of the sending abusive or inappropriate text messages and or taking inappropriate images. Staff may use their mobile phones in the staff room or outside of formal school time. See the mobile phone policy.

The sending of abusive or inappropriate text messages by children is forbidden.

### **School Website**

The school website is maintained and kept up to date by all permanent school staff through the resource TA.

The headteacher ensures that the content is accurate and appropriate to the needs of the school community.

No personal information about any member of the school community will be published on the website.

Written permission from parents or carers will be obtained before photographs of pupils or pupil names are published on the website.

### **Consent Forms**

A consent form, which covers permission to access the Internet, will be issued to parents and carers.

This will contain the acceptable use of internet guidelines. Parents and carers will be required to sign the consent form and where appropriate pupils will also be required to sign an acceptance of both the acceptable use guidelines and the e-safety policy. The signed consent form must be returned to the school for pupil access to the Internet to be permitted.

The school will keep an up-to-date record of all staff and pupils who are granted Internet access.

## **Cyber Bullying**

Cyber bullying is when the Internet, mobile phones or electronic devices are used intentionally to hurt or embarrass another person. As with any other type of bullying, Cyber bullying only occurs if a person is **repeatedly** tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another person using digital technology.

Cyber Bullying will not be permitted by the school. This is as important to the school as any other type of bullying and thus is an integral part of the school Anti Bullying Policy.

## **Staff use of ICT**

When using ICT staff must act in a professional manner at all times. Staff are not permitted to contact children via text, social networking sites, email or any other form or ICT. Staff are instructed to report approaches to them by pupils or families from the school environment. School business must not be discussed on social networking sites.

## **Non Compliance**

The headteacher will ensure that the e-safety policy is implemented and compliance with the policy monitored.

Pupils and staff will be made aware that Internet traffic can be monitored and traced to the individual user, thus appropriate use and professional conduct is essential.

All members of staff including teachers, supply staff, classroom assistants and support staff, will be provided with access to a copy of the school e-safety policy. Staff development in safe and responsible internet use will be provided as part of the continuing professional development programme.

Where incidents occur, due to non-compliance with the school e-safety policy, these will be reported to a delegated senior member of staff, in this instance Mr J Wallace.

Should it become necessary to prohibit the use of internet resources for a pupil then parents or carers will be involved so that a partnership approach can be used to resolve any issues. This could include practical sessions and suggestions for safe internet use at home.

If it is discovered that children are accessing social network sites in an inappropriate manner, and they are not old enough to do so, the headteacher has the right to contact this provider and request that the account be suspended or shut down.

Any issues relating to staff misuse of the internet must be referred to the headteacher; Should sanctions be required these should be commensurate with the offence and may involve recourse to the schools disciplinary policy and advice from the Human Resources department.

## **Risk Assessment**

Some material available on the Internet is unsuitable for pupils. Methods to identify, assess and minimise risks will be reviewed regularly. The school will take all reasonable precautions to ensure that pupils access only appropriate material.

However, due to the nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

N Copp - June 2017