REDLANDS PRIMARY SCHOOL

E-SAFETY POLICY

Introduction

At Redlands the purpose of internet use is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. We recognise that the internet is an essential element in 21st century life for education, business and social interaction, and that the school has a duty to provide pupils with quality internet access as part of their learning experience. Pupils use the internet widely outside school and will therefore need to learn how to evaluate internet information and to take care of their own safety and security.

1. **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 through emailing, blogs etc;

- 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 with support services, professional associations and colleagues;

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

- exchange of curriculum and administration data with the DfE;

- access to learning wherever and whenever convenient.

2. **The internet enhancing learning**

- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for any internet use.

- Internet access will be planned to enrich and extend learning activities.

- Staff will guide pupils to 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.

3. **Evaluating internet content**

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Internet Service Provider via the ICT subject leader or network manager.

- The school should ensure that the use of internet-derived materials by staff and by pupils complies with copyright law.

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

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

4. **Managing Internet Access**

- The security of the school ICT systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the CSA.
- The ICT subject leader / network manager will review system capacity regularly.

5. **Use of Email**

- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Whole-class or group email addresses should be used at Key Stage 2 and below.
- Excessive social email use can interfere with learning and may be restricted.
- The forwarding of chain letters is not permitted.

6. **Published Content – School Website**

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Pupils' work can only be published with the permission of the pupil and parents.
- Newsgroups will not be made available to pupils unless an educational requirement for their use has been demonstrated.

7. **Social networking and personal publishing** .

- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, email address, names of friends, specific interests and clubs etc.
- To prepare them for possible safe future use of social networking sites, pupils are advised not to place personal photos on any social network space. They must consider how public the information is and consider using private areas. Advice is given regarding background detail in a photograph which could identify the student or his/her location, e.g. house number, street name, school, shopping centre.
- Teachers are advised not to run social network spaces for children on a personal basis, nor to communicate with children and/or parents or carers via social networking sites.
- Redlands is aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments. Advice about how to respond to this type of cyber-bullying is given as part of our anti-bullying policy.

8. **Emerging technologies and mobile phones**

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

- Mobile phones will not be used during lessons, unless by the teacher for educational purposes or during a lockdown.
- The sending of abusive or inappropriate text messages is forbidden.

9. Internet Access

- 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 may be withdrawn.
- At Key Stage 1, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Pupils will not be issued individual e-mail accounts, but will be authorised to use a group/class e-mail address under supervision as appropriate.

10. Risk Assessment

- 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 and all the necessary firewalls and other security procedures will be in place.
- 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 is also monitored.

11. E-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.

12. Internet used across the community

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

13. Communications Policy

- Pupils will be informed that internet use will be monitored.
- Instruction in responsible and safe use should always precede internet access.
- A module on responsible internet use will be included in the PSHE, Citizenship or ICT programmes covering both school and home use.

14. Employees

- All staff must accept the terms of the staff code of conduct which refers to responsible use of the internet and social networking sites.
- All staff will be given the e-Safety Policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff development in safe and responsible internet use and on the e-Safety Policy will be provided as required.

15. Parental Support

- Parents' attention will be drawn to the e-Safety Policy in newsletters and on the school's website.

Policy Review Date: Summer 2020