RACK HOUSE PRIMARY SCHOOL

E-SAFETY POLICY

Contents

1 Introduction 3
2 Core Principles of Internet Safety 3
3 Why is Internet use Important? 3
4 Ethos 3
5 Roles and Responsibilities 4
6 Teaching and Learning 5
  Benefits of Internet Use for Education 5
  The Internet Enhancing Learning 5
7 Managing Content 5
  Internet Access and Content 5
  Managing Website Content 6
8 Communication 6
  Managing E-mail 6
  Social Networking and Chat Rooms 7
 Mobile Phones 7
9 Filtering 7
10 Authorising Internet Access 7
11 Assessing Risks 8
12 Communication of Policy 8
  Pupils 8
  Staff 9
  Parents/Carers 9
13 Dealing with Complaints 9

1 INTRODUCTION

This policy has been developed to ensure that all adults at **Rack House Primary** are working together to safeguard and promote the welfare of children and young people. E-Safety is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

Young people have access to the Internet from many places, home, school, friends' homes, libraries and in many cases mobile phones. Schools have 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. This policy is designed to ensure safe internet use by pupils in school, but also while on-line at home etc.

2 CORE PRINCIPLES OF INTERNET SAFETY

This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities by using ICT, whilst minimising any associated risks. It describes actions that should be put in place to redress any concerns about child welfare and safety as well as how to protect children, young people and staff from risks and infringements.

The Headteacher or, in their absence, the authorised member of staff for e-safety **(ICT subject leader/Site Manager)** has the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care.

3. WHY IS INTERNET USE IMPORTANT?

The internet is an essential element in 21st century life for education, business and social interaction and the school has a duty to provide children and young people with quality access as part of their learning experience.

The purpose of internet use in school is to help raise educational standards, promote pupil achievement, support the professional work of staff as well as enhance the school's management information and business administration systems.

4. ETHOS

It is the duty of the school to ensure that every child and young person in its care is safe. This expectation also applies to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and its everyday practice and procedures.

All staff have a responsibility to support e-Safe practices in school and all pupils need to understand their responsibilities in the event of deliberate attempts to breach e-safety protocols.

Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will dealt with in accordance with the school's Anti-Bullying and Behaviour Policy.

Complaints related to child protection will be dealt with in accordance with the school's Safeguarding Policy.

5 ROLES AND RESPONSIBILITIES

All staff At Rack House Primary School should be included in E-Safety training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.

A Designated Member of Staff for E-Learning/Safety is identified and receives appropriate on-going training, support and supervision and works closely with the Designated Person for Safeguarding.

All temporary staff and volunteers are made aware of the school's E-Learning/Safety Policy and arrangements.

A commitment to E-Safety is an integral part of the safer recruitment and selection process of staff and volunteers.

There is a senior member of the school's leadership team who is designated to take the lead on E-Learning/Safety within the school.

Procedures are in place for dealing with breaches of e-safety and security and are in line with Local Authority procedures.

All staff and volunteers have access to appropriate ICT training.

The Designated Member of Staff for E-Learning/Safety will:

- Act as the first point of contact with regards to breaches in e-safety and security.
- Liaise with the Designated Person for Safeguarding as appropriate.
- Ensure that ICT security is maintained.
- Attend appropriate training.
- Provide support and training for staff and volunteers on E-Safety.
- Ensure that all staff and volunteers have received a copy of the school's Acceptable Use of ICT document.
- Ensure that all staff and volunteers understand and aware of the school's E-Learning/Safety Policy.
- Ensure that the school's ICT systems are regularly reviewed with regard to security.
- Ensure that the virus protection is regularly reviewed and updated.
- Discuss security strategies with the Local Authority particularly where a wide area network is planned.
- Regularly check files on the school's network.

6 TEACHING and LEARNING

Benefits of internet use for education

The internet is a part of the statutory curriculum and a necessary tool for staff and children and young people and benefits education by allowing access to world - wide educational resources including art galleries and museums as well as enabling access to specialists in many fields for pupils and staff.

Access to the internet supports educational and cultural exchanges between students world - wide and enables pupils to participate in cultural, vocational, social and leisure use in libraries, clubs and at home.

The internet supports professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of curriculum and administration data with the Local Authority and DCSF.

The Internet enhancing learning

Internet use will be planned to enrich and extend learning activities and access levels will be reviewed to reflect the curriculum requirements and age of the children and young people.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Children and young people will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Children and young people will be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be taught research techniques including the use of subject catalogues and search engines and encouraged to question the validity, currency and origins of information.

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

7 MANAGING CONTENT

Internet Access and Content

Developing good practice in internet use as a tool for teaching and learning is essential. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the children and young people.

Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for internet use. Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupil’s age and maturity.

Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening, following the school motto ‘If you see something you do not like, tell an adult.’

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

Annually, all pupils along with parents/carers will be asked to read, accept and sign an acceptable usage policy (AUP) explaining how they will abide by the policies use of safe Internet access. Pupils who do not return these forms will not be allowed Internet access in school until they do so.

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

Managing Website Content

Editorial guidance will ensure that the school’s ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. The headteacher or nominated person will have overall editorial responsibility and ensure that all content is accurate and appropriate.

The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils’ home information will not be published.

Website photographs that include pupils will be selected carefully and will not enable individual pupils to be identified by name.

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

Staff may use photographic or video technology to capture to support school trips and appropriate curriculum activities.

8. COMMUNICATION

Managing E-mail

Pupils may only use approved e-mail accounts on the school system.

Pupils must immediately tell a teacher if they receive offensive e-mail.

Pupils must not reveal details of themselves or others in e-mail communication, such as addresses or telephone numbers, or arrange to meet anyone.

Individual e-mails for pupils in KS2 can be set up with a generic password known to the class teacher.

E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Incoming e-mail should be monitored and attachments should not be opened unless the author is known.

Social Networking and Chat Rooms

Pupils will be taught about how to keep personal information safe when using online services. Each year group will have specific ICT lessons dedicated to e-safety every term.

The use of online chat is not permitted in school, other than as part of its online learning environment and access to social networking sites will be blocked unless a specific use is approved.

Pupils will be advised never to give out personal details of any kind which may identify them or their location and are advised to use nick names and avatars when using social networking sites.

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

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

Pupils and parents should be made aware that some social networks are not appropriate for children of primary school age

Staff will not exchange social networking addresses or use social networking sites to communicate with pupils.

Mobile Phones

Mobile phones of pupils are not permitted within the school. In exceptional circumstances a letter may be written by a parent/carer to the head teacher explaining why one is needed. The head teacher will make the final decision on the matter.

Appropriate use of mobile phones will be taught to pupils as part of their e-safety learning.

9 FILTERING

The school will work in partnership with parents/carers, the Local Authority, the DCFS and the Internet Service Provider to ensure systems to protect pupils and staff are reviewed and improved regularly.

If staff or pupils discover unsuitable sites, the URL **(**website address) and content must be reported and the ICT Subject Leader**.**

Filtering methods will be selected by the school in conjunction with the LA and will be age and curriculum appropriate.

10 AUTHORISING INTERNET ACCESS

All staff must read and sign the school's 'Staff Code of Conduct for ICT' before using any school ICT resources and any staff not directly employed by the school will be asked to sign the school's 'Acceptable Use of ICT Resources' document before being allowed internet access from the school site.

The school will maintain a current record of all staff and pupils who are allowed access to the school's ICT systems.

The school will maintain a record of pupils whose parents/carers have specifically requested that their child be denied internet or e-mail access.

Parents/carers will be asked to sign and return the school's form stating that they have read and understood the school's 'e-safety' rules and give permission for their child to access ICT resources.

Staff will supervise access to the internet from the school site for all pupils.

11 ASSESSING RISKS

Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. Staff should be aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and allow a new route to undesirable material and communications.

In common with other media such as magazines, books and video, some material available through the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to international scale and linked nature of Internet content, it is not always possible to guarantee that unsuitable material may never appear on a school computer. Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences of Internet access.

Emerging technologies will be examined for educational use and a risk assessment will be carried out before use in school is allowed and methods to identify, assess and minimise risks will be reviewed regularly.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.

The headteacher and ICT subject leader will ensure that the E-Safety Policy is implemented and compliance with the policy is monitored.

Access to any websites involving gambling, games or financial scams is strictly forbidden and will be dealt with accordingly.

12 COMMUNICATION OF POLICY

Pupils

Rules for Internet access will be posted in all rooms where computers are used.

Responsible Internet use, covering both school and home use, will be included in the ICT curriculum.

Pupils will be instructed in responsible and safe use before being allowed access to the Internet and will be reminded of the rules and risks before any lesson using the Internet.

Pupils will be informed that internet use will be closely monitored and that misuse will be dealt with appropriately.

Each year group will have specific ICT lessons dedicated to e-safety every term. Responsible Internet use and e-safety will be included in the curriculum covering both school and home use. This will include the necessity of keeping personal information safe, how to use mobile technologies appropriately and using online communication appropriately.

Staff

All staff will be given the School 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.

All new staff will be given a copy of the policy during their induction.

Staff development in safe and responsible use of the internet will be provided as required.

Parents/Carers

Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure 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 includes an e-safety workshop every term informing parents/carers about safe Internet use at home. Parents/carers attending the workshop will be referred to organisations such as Child Exploitation and Online Protection (CEOP) and websites for parents and carers (www.thinkuknow.co.uk)

13 DEALING WITH COMPLAINTS

The school's designated person for e-safety will be responsible for dealing with complaints and any complaint concerning staff or pupil misuse of the internet must be reported to the head teacher immediately.

Pupils and parents/cares will be informed of the complaints procedure.

Parents/carers and pupils will work in partnership with the school staff to resolve any issues.

There may be occasions when the school must contact the police. If appropriate, early contact should be made to discuss strategies and preserve possible evidence.