E Safety Policy

Our E-Safety Policy has been written by Thornhill Primary School. It has been agreed by the Senior leadership team and approved by the Governing Body. The e-Safety Policy will be reviewed annually.

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 information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

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

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- 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 and professional associations;
- exchange of curriculum and administration data with the Local Authority and DCSF; access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes 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.
- Staff should guide pupils in on-line activities that will support 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.

Authorised Internet Access

- All staff and pupils are granted Internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be sent the pupil e safety agreement.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the e-safety coordinator or network manager.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- 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 personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school
- Access in school to external personal e-mail accounts are blocked.

- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Staff may contact pupils via approved school email accounts as this can be monitored by the e-safety coordinators. This should be within school hours and only be about school related work.

Social Networking

- The LA blocks/filters access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised about the rules of using social networking sites and we aim to educate children about the legal implications of improper use.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.
- Staff are advised to use security settings within their social networking site to restrict information to only known friends. Staff can see the e-safety coordinator for help with this.
- It is not appropriate for staff to share work-related information whether written or pictorial via a social networking site.
- Under no circumstance should comments be made about other staff, pupils, parents/carers or school procedures on the Internet. Staff members should respect the privacy and the feelings of others. This could be deemed a disciplinary offence.
- Staff should not be friends with parents, carers or pupils on social networking sites. In situations where staff are friends with parents in a social capacity, it may be necessary for separate accounts to be held.
- If a member of staff believes something has been written which gives rise to concerns within this, or any other policy this must be discussed with the e-safety coordinator and a member of the Senior Leadership team.
- If a message or 'friend request' is received by a member of staff from a parent, carer or pupil, staff should ignore any messages and reject the request. Under no circumstances should staff reply as this can result in online information becoming available to others. Staff should inform the school e-safety coordinator about any messages or friends requests received from parents, carers or pupils.

Filtering

The school works in partnership with the Local Authority and the Internet Service Provider to ensure filtering systems are as effective as possible.

Video Conferencing

- Video conferencing will always be done through an approved provider and will always be fully supervised in school.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will use the school phone where contact with pupils is required.
- Our schools recommends that pupil mobile phones are not brought into school unless in extreme circumstances, and with prior agreement. These will then be stored securely in the school safe.

Published Content and the School Web Site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The e-safety coordinator, the Head teacher and Assistant Head Teacher, will take editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- 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 Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection is installed and updated regularly.

Protecting Personal Data

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

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor RMBC can accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling 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 e-safety coordinator and a member of the school SLT.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer, CEOP, to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils

- Rules for Internet access are posted in all networked rooms.
- Pupils are informed that Internet use will be monitored.
- Pupils have read and signed a safe computer use agreement.

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.
- Staff will have read and signed the Staff Systems Code of Conduct.

Parents

Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site. They will have been asked to read our safe internet use rules.