Kirton Primary School e-safety and Acceptable Use Policy

This policy has been agreed by the senior management and approved by governors.

The purpose of Internet use in schools is to raise educational standards, to promote pupil achievements, to support the professional work of staff and to enhance the schools management information and business administration systems.

1. Teaching and Learning
1.1 Why the Internet and digital communications are important

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

1.2 Internet use will enhance learning by providing

- Access to world-wide educational resources.
- Educational and cultural exchanges between pupils world wide.
- Cultural, vocational, social and leisure use in libraries, clubs at home.
- Access to experts in many fields for pupils and staff.
- Staff professional development through national developments, educational materials and good curriculum practice.
- Communication with support services, professional associations and colleagues.
- An exchange of curriculum and administration data with the LA and DfE. Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Opportunities for staff to guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

- Showing pupils how to publish and present information to a wider audience. (Staff must ensure that the use of internet derived materials by staff and pupils complies with copyright laws.)
- Teaching pupils to acknowledge the source of information and to respect copyright when using internet material in their own work.
- Encouraging pupils to question the validity and origins of information and look for alternative sources of information for comparison purposes.

1.3 Safe Use
- The school internet access will be designed expressly for pupils' use and will include filtering appropriate to their age.
- Pupils will be taught what is acceptable and what is not and given clear objectives for internet use.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Leader.
- The use of mobile phones is not permitted during school times.

1.4 Pupils will be taught how to evaluate Internet content
The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed or any consequences rising from internet access.
Pupils should be taught what to do if they experience material that they find uncomfortable or threatening.

2. **Managing Internet Access**
   ### 2.1 Information system security
   - School ICT systems security will be reviewed regularly.
   - Virus protection will be updated regularly.
   - Security strategies will be discussed with the Local Authority.
   - Wireless networks will be protected to the best of our ability from outside use
   - Staff and students will change their passwords on a periodic basis
   - Staff and students will log out of the system when not in use

2.2 Email

The government encourages the use of email as an essential means of communication and should be used appropriately.

- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in email communication.
- Access in school to external personal email accounts may be blocked.
- Email sent to an external organization should be written so as not to cause offence or anxiety.
- The forwarding of chain letters is banned.
- Staff and children's email may be checked.

2.3 The use of chat rooms.

- Pupils will not be allowed access to public chat rooms or unregulated chat rooms.
- Children should use only regulated educational chat environments. This use will always be supervised and the importance of chat room safety emphasised.
- Emerging technologies will be examined for educational benefits and a risk assessment will be carried out before use in school is allowed.

2.4   Published content and the school web site

- Staff or pupil personal contact information will not be published.
- The contact details given online should be the school office.
- The Governing Body takes overall editorial responsibility for the website to ensure that published content is accurate and appropriate.

2.5 Publishing pupils' images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified.
- Pupils' full names will not be used anywhere on a school web site or other on-line space, particularly in association with photographs.

2. 6 Managing Filtering

Levels of access and supervision may vary according to the pupils' age and experience. Internet access must be appropriate for all members of the school community from the youngest pupil to teacher and administration staff.

- The school will work in partnership the LA and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

- The ICT leader will work with the Internet service Provider to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported.

3. Policy Decisions

3.1 Authorising Internet Access

The school will keep a record of all staff and pupils who are granted internet access.

- At Foundation stage and Key Stage One, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be informed that pupils will be provided with supervised internet access
-

3.2 Assessing Risks

In common with other media such as magazines, books and videos, some materials available via the internet are unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material.

- The use of computer systems without permission for the inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimize risks will be reviewed regularly.

4. Communications Policy

4.1 Introducing this policy to pupils

- Students will be made aware of e-safety rules
- Students and parents will be informed that network, internet and ICT use will be monitored.

4.2 Staff and this policy

- All staff including teachers, supply staff, classroom assistants, support staff and office staff will be given access to this policy.
- Staff development in safe and responsible internet use and on school internet policy will be provided as required.
- Staff must only use their own log in and password and not share them with others.

Appendix A

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety and acceptable use policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.

- I will ensure that my information systems use is compatible with my professional role.

- I understand that school information systems, including social networking sites, may not be used for private purposes without specific permission from the headteacher.

- I understand that it would be unprofessional to make negative or inappropriate comments concerning members of the school community or the management of the school in a public arena.

- I understand that the school may monitor my information systems and internet use to ensure policy compliance.

- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.

- I will respect confidentiality and not open or delete another person's files without their express permission.

- I will not install any software or hardware without permission.

- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.

- I will respect copyright and intellectual property rights.

- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.

- I will ensure that any electronic communications with pupils are compatible with my professional rôle.

- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including internet access, the interception of e-mail and the deletion of inappropriate materials to check whether there has been unauthorised use of the school's information system, or the system has been being used for criminal purposes or used for storing unauthorised or unlawful text, imagery or sound.