Craneswater Junior School
e-Safety Policy

Craneswater Junior School believes that the teaching and learning and use of information and communication technologies in schools is an essential element of 21st century education. Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used.

The school has a duty to provide pupils with quality internet access as part of their learning experience and internet use is part of the statutory curriculum. Craneswater Junior School takes the safety of all children and adults very seriously and this policy is written as part of the school's commitment to keep pupils and staff safe. It should be read in conjunction with the school's policies for Computing, Acceptable Use, Anti-bullying, Safeguarding and Child Protection.

We recognise that e-Safety encompasses not only Internet technologies, but also electronic communications, such as mobile phones and wireless technology.

1. What does electronic communication include?

- **Internet collaboration tools:** social networking sites and web-logs (blogs);
- **Internet research**: websites, search engines, and web browsers;
- **Mobile phones**
- **Internet communications**: email and IM;
- **Webcams and video conferencing;**
- **Wireless games consoles.**

This e-Safety Policy should recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for others.

These risks to e-safety are caused by people acting inappropriately and even illegally.

What are the risks?

- Receiving inappropriate content;
- Predation and grooming;
- Requests for personal information;
- Viewing 'incitement' sites;
- Bullying and threats;
- Identity theft
- Publishing inappropriate content;
- Online gambling;
- Misuse of computer systems;
- Publishing personal information;
- Hacking and security breaches;
- Corruption or misuse of data.

We recognise that this is not an exhaustive list. No policy can protect pupils without effective implementation. It is essential that staff remain vigilant in planning and supervising appropriate, educational computing experiences.

1. Responsibility

The Computing Team are responsible for producing and promulgating the e-safety policy within school. To achieve this they will liaise with the Designated Lead for Safeguarding Children.

It is the responsibility of each member of staff to read and understand the policy and to ensure compliance. Staff are required to read and sign the Acceptable Use policy each year.

Class teachers are required to remind children of the school's e-safety rules, "Think & Click". Children will be responsible for ensuring their own adherence to "Think & Click" e-safety rules (Appendix 1).

The school will reassess the e-safety policy regularly and it will be reviewed 3 yearly unless changes or developments in emerging technologies dictate an earlier date is necessary.

The e-safety policy will be made available to all stakeholders via the school website. The e-safety coordinator (Computing Manager) should maintain the e-Safety policy, manage e-safety training and keep abreast of local and national e-safety awareness campaigns.

The school's internet use will be designed expressly for pupil use and will include filtering appropriate to the age of the pupils. Internet filtering is provided by the Local Authority. The Local Authority is also responsible for monitoring internet use within the school.

2. Teaching and learning

2.1 Why is Internet use important?

The rapid developments in electronic communications are having many effects, some profound, on society.

- 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 functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning. However misuse may result in the loss of this entitlement.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

2.2 How will the school use the Internet to enhance learning?

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Filtering will be provided by the Local Authority.
- Pupils will be taught what Internet use 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.
- Pupils will not be allowed to access the internet in school without adult supervision.

2.3 How will pupils learn how to evaluate Internet content?

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop skills in selection and evaluation. Information received via the Internet, e-mail or text message requires good information handling skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues present with books or TV may be missing or difficult to read.

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- 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.

2.4 Access to inappropriate Internet content

In a perfect world, inappropriate material would not be visible to pupils using the Internet, but this is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. The policy distinguishes between accidental and deliberate access.

2.4.1 Accidental Access

Pupil should immediately close the page and report the incident to the adult supervising their internet use. The adult supervisor should report the incident to a member of the Computing team who will pass on a report to the Local Authority if necessary. The incident should also be recorded in the e-safety log.

2.4.2 Deliberate Access

Deliberate access to inappropriate material, by any member of the school community, is a serious offence and should be reported to a member of the senior management team. The incident must also be logged in the e-safety folder at the earliest opportunity. Staff should use professional judgement when dealing with children who make unsuccessful attempts to access inappropriate material.

3. Systems Security

3.1. How will information systems security be maintained?

The Computing team will regularly review the security of all the school information systems.

3.2. Local Area Network Security

- All network users will be issued with a unique network user name. Users should only log on to the network using their own network name.
- Pupils have limited network access privileges. These will be periodically reviewed by the ICT team. Access to pupil accounts is not password protected.
- Staff have greater network access privileges. They will be issued with passwords to control access to their accounts. It is important that these passwords are kept secure, in particular they must not be revealed to pupils.
- Virus protection will be updated regularly.
- Pupils will not be able to connect portable media to the network.
- Staff are able to connect portable media to the network. It is the responsibility of all members of staff to ensure that all files introduced to the network are free from viruses and other malicious software.
- Executable files can only be installed on the network by the System Administrators.
- Files held on the school's network will be subject to monitoring and inspection.
- Data held on the network will be backed up in accordance with the IT Back Up procedure.

3.3. E-mail Security

- Pupils may only use approved e-mail accounts.
- All communication using the school e-mail system is subject to monitoring.
- 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.
- Staff have access to a school e-mail address provided by the Local Authority. It is the responsibility of staff to ensure that they keep their login details secure. All e-mail sent over the system is subject to monitoring.
- 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.

3.4. Messaging Security

- Access to external instant messaging systems (e.g. MSN, AIM) is prohibited and as far as practicable will be blocked.

- Several websites and applications that are used to support the Computing curriculum have messaging facilities that are intended to facilitate collaboration. These facilities can be very useful. Teachers must emphasise to all pupils that the messaging facilities must be used responsibly. In particular messaging should not be used during lessons for any purpose other than to enable children to work together on projects. All children must report receipt of inappropriate messages to a teacher.

3.5. Social Networks

- Access to Social Network sites (e.g. MySpace, Facebook) is prohibited within school.

3.6. Mobile Phones

- Pupils should be strongly discouraged from bringing mobile phones into school. Pupils who do bring mobile phones into school must leave them in the school office at the start of the school day and collect them at the end of the day.

4. How will published content be managed?

- Data may be published electronically on both the school public website and within the Learning Platform.

4.1 Public Website

- All content should be submitted to the website administrator for inclusion.
- All content authors will be responsible for complying with copyright legislation when including third party material.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

4.2 Publication of pupil's images and work

- The school will publish, selected examples of work and images of the children (both still and moving) unless parents have specifically and explicitly withheld permission for such publication.
- Images 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 in association with photographs.

5. Social Networking

- The school will block / filter all access to social networking sites;
- All school staff should be aware that, despite the majority of children not meeting age restrictions on popular networking sites, they may still access these and others with no recommended age restrictions.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location, such as real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place any personal photos on any social network space.
- Pupils should be made aware of the longevity of pictures or comments posted onto networking sites.

6. Cyberbullying

- Cyber bullying will be treated in the same way as any other bullying incident whether it takes place inside or outside school (See School Bullying Policy).
- E-safety and cyberbullying are addressed within the PSHE curriculum.

7. Personal Data

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

8. Policy Decisions

8.1. How will Internet access be authorised?

The school will allocate internet access for staff and children on the basis of educational need. Pupil use of the internet will be under adult supervision. Class teachers have the ability to withhold access in cases of misuse.

- All staff must read and sign the 'Acceptable Use Policy'.
- Children will agree and sign the 'Think and Click' policy.
- All children and parents will be aware of the E-Safety rules.

8.2. How will e-safety incidents be recorded?

Any incident relating to e-safety will be recorded with reference to behaviour and / or safeguarding policies.

8.3. How will e-safety complaints be handled?

- Any complaint about staff misuse must be referred to the Head teacher.
- Any complaint concerning internet use will follow the school's complaints procedure.
- Sanctions within the school will be in accordance with the school's behaviour policy.

9. Communications.

- Electronic copies of e-safety related documents are held in the e-safety folder on the Staff drive on the school network.
- E-Safety rules 'Think and Click' will be posted in rooms with Internet access.
- Pupils will be informed that network and Internet use will be monitored.
- Staff will be consulted in staff meeting and will sign the Staff 'Acceptable Use Policy'
- The E-safety policy will be ratified by the Governing body.
- All children will read and sign the 'Think and Click' poster. A copy of the class's signed poster should be displayed in each classroom.
- An e-safety module covering both school and home use will be included in the PSHE curriculum.
- Parents will be informed of E- safety using the school's newsletter and / or via the parents' forum.