Crofton Infants' School
E-Safety Policy

Education – Pupils

The education of pupils in e-safety is an essential part of the school's role to keep children safe from harm. Children and young people need the help and support of all adults to recognise and avoid e-safety risks and build their knowledge and understanding.

E-Safety education will be provided in the following ways:

- A planned e-safety programme will be provided as part of PSHCE and ICT lessons. As ICT is integrated throughout the curriculum e-safety will be reinforced whenever applicable. This will cover both the use of ICT and new technologies in school and outside school.
- Key e-safety messages will be addressed through a planned programme of lessons based on
  'Hector's World', 'You Think You Know' and 'Roar Educate'.
- Pupils will be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- In Foundation Stage and KS1 pupils will be helped to understand the principles of our Acceptable Use Policy (AUP) but will not be asked to sign an AUP.
- Pupils will be taught to acknowledge the sources of information they use and to respect copyright when using material accessed on the Internet.
- Rules for use of ICT systems and the Internet will be posted in all rooms.
- Staff will be made aware that they are role models in their use of ICT, the Internet and mobile devices.

Education – Parents/ Carers

Parents and carers may have a limited understanding of e-safety risks and issues, yet they play an essential role in the education, monitoring and regulation of their children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the Internet and are often unsure about what they would do about it. "There is a generational digital divide." (Byron Report).

The school will:

- Provide written e-safety information for parents.
- Include links to 'Hector's World' and 'You think You Know' on the school's website.

Education & Training – Extended Schools

- After school clubs may have access to the schools ICT systems. Pupil use will be monitored at all times by staff at the clubs. Children are always made aware of e-safety issues.

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their roles and responsibilities.
A planned programme of formal e-safety training will be made available to staff.

- E-Safety training for staff will be carried out annually.

- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies (AUP).
- The school e-safety policy and any updates will be presented to and discussed by staff in staff meetings or during INSET days. This will happen at least once in a twelve month cycle.
- The e-safety coordinator (or other nominated person) will provide advice, guidance and training, as required.

Education & Training – Governors

- The school has a named governor with responsibility for e-safety. Feedback from e-safety courses will be provided and training needs identified and provided as appropriate.
- The school's e-safety governor will liaise with the SMT and e-safety coordinator to ensure governors are kept up-to-date with e-safety training.
- Any issues regarding e-safety will be reported immediately to the e-safety governor.

Curriculum

E-Safety will be a focus in all areas of the curriculum and staff will reinforce e-safety messages in the use of ICT across the curriculum.

- Pupil use of the Internet at school must be supervised at all times.
- When using the Internet, links may be created as 'Favourites' in an Internet browser. All links and searches are subject to the exclusions created by the Yorkshire and Humberside Grid for Learning (YHGfL).
- When using search engines, staff will be vigilant in monitoring the websites pupils visit.
- In all lessons pupils will be taught to be critically aware of the materials and content they access online and be guided to validate the accuracy of information.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.

When using communication technologies:

- Staff will be provided with individual school email addresses for educational use. The official school email service may be regarded as safe and secure. Staff should therefore use only the school email service to communicate with others when in school or using school systems (for example, by remote access).
- Users need to be aware that email communications may be monitored.
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Reports should be made to the e-safety coordinator or SMT in accordance with the school policy and users must not respond to any such email.
- Any digital communication between staff and pupils or parents/carers must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging, public chat and social networking programmes must not be used for these communications.
- Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Technical – infrastructure/equipment, filtering and monitoring

The school will ensure that the school infrastructure/network is as safe and secure as possible and that policies and procedures approved within this policy are implemented. The SMT will ensure that relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets any e-safety technical requirements and Acceptable Use Policy and any relevant Local Authority e-safety policy and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling are securely located and physical
- access restricted.
- Users have clearly defined access rights to the school ICT systems.
- Pupils do not have individual passwords to access the school system. Each class has its own log-in, which is not currently password protected. Pupils' use of ICT is closely monitored by the class teacher or teaching assistant who is working with them.
- Staff have their own individual login which is password protected. They are made aware that they are responsible for any network usage while they are logged on to a particular computer.
- Visitors to school, such as supply teachers, students or parent helpers, will be issued with a guest username and password as needed.
- Users are responsible for the security of their username and password and will not allow other users to access the systems using their log-in details. Any suspicion or evidence that this is known to others will be reported immediately to the e-safety coordinator or SMT.
- The 'master/administrator' passwords for the school ICT system, used by the Network Manager, are available to the SMT and kept in a
- secure place.
- Any filtering issues will be reported immediately to the SMT or e-safety coordinator and then to ICT4C.
- Requests from staff for sites to be removed or added from the filtered feed will be considered by the SMT. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the SMT or e-safety coordinator.
- Appropriate and relevant security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices and all other ICT equipment from accidental or malicious attempts which might threaten the security of the school systems and data.
- As specified in the AUP, teacher laptops and other portable devices will be used by the named member of staff for educational purposes only.
- As agreed in the AUP, staff will not install programmes or hardware on school workstations or portable devices without the consent of the SMT or e-safety coordinator.
- As agreed in the AUP, the use of removable media (for example, memory sticks /CDs/DVDs) by users on school workstations or portable devices is permitted, providing they are virus checked prior to use. Personal data relating to pupils or staff will only be carried on removable media or sent over the internet with the permission of the SMT. Personal data must always be stored securely.

The school infrastructure and individual workstations are protected by up to date virus software.

Crofton
Infant's
School
September
2014