Deneholm Primary School

E-safety Policy

Deneholm Primary School

E-safety Policy

Statement of Intent

We are committed to providing a caring, friendly and safe environment for all our pupils so they can learn in a relaxed and secure atmosphere. Allowing them to gain the knoweldge to enable to keep them safe when using any form of ICT.

Empowering children to be e-safe

In order to fulfill the e-safety element of our vision statement for ICT, our policies and practices focus on:

"a model of empowerment; equipping children with the skills and knowledge they need to use technology safely and responsibly, and managing the risks, wherever and whenever they go online; to promote safe and responsible behaviours in using technology both at school and in the home and beyond."
Safeguarding children online – Becta February 2009

Entitlement

All pupils have an entitlement to the following:

- Staff commitment to enable development of their full potential at all times.
- Learning experiences and lessons that will stimulate, interest, challenge, inform, excite and encourage through partnership and dialogue with adults and other children.
- Skilled, well-prepared and informed teachers and support staff who firmly believe that Every Child Matters.
- An entitlement beyond subject teaching that includes extra curricular activity and opportunities for individual challenge.

Teaching and Learning

ICT offers us the opportunity to transform education, help pupils fulfill their potential and raise standards.

Using the Internet

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum. The school Internet access is designed for use by all learners in the school community: pupils, staff, governors, parents, carers and friends. It will include filtering appropriate to the age and experience of the user, set up by, and maintained by the ICT coordinator. 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, evaluation and application. Pupils will learn how to publish and present information to a wider audience.
The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught the importance of cross-checking information before accepting its accuracy. Users will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector.

Managing Internet Access

Security of our ICT systems is managed by the ICT coordinator. Children can be banned from using the Internet if they breach the Acceptable Users Policy that all children have agreed to.

Managing Filtering

The ICT coordinator works with E2BN Protex to manage, review and improve filtering on our systems. If any user comes across unsuitable on-line materials, it must be reported to the e-Safety coordinator and the ICT coordinator. It is then their responsibility to ensure the ICT Service are informed.

Published content and the school web site

Staff, pupil or governor personal contact information will not be published. The Headteacher and ICT coordinator takes overall editorial responsibility for the website. However, it would be unrealistic for them to check every posting for submission. Therefore, only staff are able to submit content; all postings must be checked by another member of staff before submission. Pupils' full names will not be used in association with photographs, where this may lead to the identification of individuals. Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site or in the press.
Permission will be sought from pupils before their work is published on the school web site. Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories, through the AUP for parents/carers. They will also be reminded at appropriate events, such as productions and sports days.

Social networking and personal publishing

Pupils and parents will be advised that the use of social networking spaces outside school brings a range of dangers to primary aged pupils. School will educate pupils in the safe use of social networking sites. However, they will not have access to them in school. Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location. Newsgroups will be blocked unless a specific use is approved by the Headteacher.

Emerging Technologies

Emerging technologies will be examined for educational benefit and if appropriate, a risk assessment will be carried out before use in school is allowed.
Staff should be aware that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications. Mobile phones or games machines will not be brought into, or used in school by pupils, without the express permission of the Headteacher, given in exceptional circumstances and only when granted in conjunction with the knowledge of parents/carers. Mobile phones will not be used during lessons by staff without the permission of the headteacher. The sending of abusive or inappropriate text messages or files while on the school premises or to members of the school community by bluetooth or any other means is forbidden. Staff will be issued with a school phone to use during day and residential visits, to make emergency contact. Under normal circumstances, their personal phone should not be used, in order to protect their future privacy. We will embrace and develop the use of emerging learning platforms (currently MyLearning), whilst continuing to reflect and act upon any potential e-safety issues that may arise.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. (See Security and Data Management Policy for further details).

Policy Decisions

Authorising Internet Access

All staff must read and sign the Acceptable User Policy for Staff, before using any ICT resource. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems. Parents will be made aware through the Pupil Acceptable User Policy, that pupils will have appropriate access to the internet. Any person not directly employed by the school will be asked to sign an Acceptable Use of school ICT resources' before being allowed to access the internet from the school site.

Assessing risks

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 of internet use. The school will audit ICT use to establish if the e-safety policy is adequate and if its implementation is appropriate and effective.

Handling e-safety complaints

Complaints of pupil internet misuse will be dealt with by an appropriate member of staff, depending on the severity of the misuse as well as the age and development of the pupil(s) involved. Pupils and parents will be informed of consequences for pupils misusing the internet. Any complaint about staff misuse must be referred to the Headteacher who will communicate with the Governor with responsibility for e-safety. The misuse must be recorded in the e-safety file. Staff should be aware they may face disciplinary action as a result of internet misuse. (See Staff AUP for further details)
Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Community use of the internet

The school will liaise with local organisations to allow members of the wider community to access school's internet/ICT equipment. Any person not directly employed by the school will be asked to sign an Acceptable Use of school ICT resources' policy before being allowed to access the internet from the school site.

Communications

Introducing the e-safety policy to pupils

Discreet teaching of e-safety will be taught as outlined on each class's long term ICT plan and also embedded at other appropriate times. E-safety rules will be posted in rooms where computers are used and pupils will be reminded of them at relevant times. Opportunities to discuss them regularly will be provided, including during an assembly with an e-safety theme, at least once a term.
Depending upon the age, experience and stage of development, staff will usually give a list of suitable, relevant sites or use a child friendly search engine when accessing the web with pupils. In addition, a

clear purpose for Internet use will always be given. Staff will be reminded that network and Internet traffic can be monitored and traced to the individual user. E-safety sites will be available for the children to use on the Learning Platform.

Enlisting parents' and carers' support

Parents' and carers' attention will be drawn to the school e-safety Policy in the school brochure, on the school website and on occasion in newsletters. The school will maintain a list of e-safety resources for parents/carers. A link from the school website and Learning Platform will also be available. The school will ask all new parents to sign the parent/carer AUP when they register their child with the school.

Resources

All teachers will keep abreast of current e-safety initiatives and resources and use these appropriately in the learning and teaching of e-safety. They will be encouraged to share effective resources with other members of staff. Staff will also be given appropriate CPD in the area of e-safety.

Implementation

Roles and responsibilities

(a) Class Teachers/ ICT coordinator

- To teach discreet lessons in e-safety as prescribed in the long term plans for ICT.
- To remind pupils of the e-safety rules as and when appropriate.
- To ensure the e-safety rules are displayed and adhered to in each classroom.
- To inform the relevant person(s) if there is a breach of e-safety.

(b) Headteacher/ ICT coordinator

- To act as the designated e-safety officer.
- To include an e-safety theme on the assembly plan each term.

(c) Governors

- The governing body has a duty to understand the need to provide suitable safeguards for pupils and the school. The safe and secure use of ICT has an impact on a number of areas of statutory responsibility for governing bodies, including Health and Safety Policy, Child Protection Policy and legal requirements for data protection and freedom of information.
- The governor with responsibility for Child Protection, also takes responsibility for e-safety.
- Any complaints about staff mis-use made to the Headteacher, will be communicated by the Headteacher to the Child Protection (e-safety) governor.
- All governors should understand their role in keeping information confidential as appropriate, and should sign and adhere to the Acceptable User Policy for Governors in order to safeguard themselves and the school.

Inclusion

All children will be taught at a level that is appropriate to their academic, emotional and physical need. Teacher planning will reflect the needs of individual pupils in regards to academic, physical, medical and sensitive issues, race, gender and faith.

We need to be particularly vigilant in ensuring that our most vulnerable children understand and follow our e-safety rules.

Safeguarding

Deneholm Primary School fully recognises the responsibility it has under section 175 of the Education Act 2002 to have arrangements in place to safeguard and promote the welfare of children.

Review

A review involving all staff will take place annually in the Spring Term 2017.