Drax Community Primary School

E-SAFETY POLICY

September 2016

Contents

E-Safety

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

Our school's e-safety policy will operate in conjunction with other policies including those for Behaviour, Bullying (including Cyber bullying), Data Protection, E-Security & Child Protection.

The Designated Person for Safeguarding (Head Teacher) will take on the role of E-Safety Coordinator.

Good Habits

E-Safety depends on effective practice a number of levels:
- Responsible ICT use by all staff and pupils.
- Sound implementation of the e-safety policy in both administration and curriculum.
- Safe and secure broadband from the Yorkshire and Humber Grid for Learning including the effective management of content filtering.

Why is Internet Use Important?

The purpose of the Internet 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. The Internet provides access to a variety of wonderful resources that can enhance and enliven learning.

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 take care of their own safety and security.

Internet use in School

- The school Internet access will be designed expressly for pupil use and includes filtering of appropriate material.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for Internet use. See Appendix 2.
- Internet access will be planned to enrich and extend learning activities.
- Staff will guide pupils in online activities that support planned learning outcomes
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

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

Authorised Internet Access

- All staff must read and sign the 'Acceptable ICT Use Agreement'.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for pupil access.
- If staff or pupils discover unsuitable sites, the URL (address), time and content must be reported to the LA via the E-Safety coordinator.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.

Email

- Pupils must not use personal email accounts in school.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- For work related communications, staff will only use their work email – not their home email. If the work email is not functioning the Headteacher will be informed and temporary permission may be given to use a personal email address for a limited time. No sensitive information eg. data, pupils names, photographs should be exchanged on a personal email account however.

Social Networking

- School will block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be encouraged not to use social-networking sites in line with age-related guidelines and will be taught how to keep themselves safe on sites.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils will be advised not to place personal photos on any social networking site.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Pupils will be advised to allow to access to known friends only and deny access to others
- School will also provide guidance for Staff regarding the use of Social Networking – specifically Facebook. This information is especially relevant to new staff and should be covered in their induction information (see Appendix 4).

Filtering

- The school will work in partnership with the LA, YHGFL and the Internet Service Provider to ensure filtering systems are as effective as possible.

Video Conferencing

- Pupils will ask permission from the supervising teacher before making or answering a video conference call.

Managing Emerging Technologies

- Pupils will not bring mobile phones and other emerging technologies in to school without prior permission from their teacher. If parents require children to bring a phone to school, this must be signed into the office on arrival and retrieved at the end of the day.
- Use of emerging technologies in school will only be for specific learning opportunities 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 by staff members unless permission has been given by the Headteacher.

Published Content on the School Web Site

- The contact details on the website will be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The Headteacher will take overall responsibility and ensure the content is accurate and appropriate.
- Pupils' full names will not be used anywhere on the website.
- Written permission from parents or carers will be obtained through the Home-School Agreement before photographs of pupils are published on the website.

Information System Security

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

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Documents containing personal data, including pupils' assessment data, will be password protected before being saved or shared.

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 the LA can accept liability for the material accessed, or any consequences of Internet access.

- The Headteacher will audit ICT use to establish if 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 Headteacher or, if involving the Headteacher, to the Chair of Governors.
- 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.

Communication of Policy

Pupils
- Rules for Internet Access will be posted in all networked rooms
- Pupils will be informed that Internet use will be monitored.
- Pupils will be taught safe Internet practice every year and will be reminded of this where applicable.

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.

Parents
- Parents' attention will be drawn to the school's E-Safety Policy in newsletters and on the school website.

Drax Community Primary School

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

➢ I will only use the school's email / Internet / Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
➢ I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
➢ I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
➢ I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
➢ I will only use the approved, secure email system(s) for any school business.
➢ It is agreed and accepted that your e-mails remain the property of the school at all times, whether they are marked private and confidential or otherwise.
➢ It is agreed and accepted that your e-mails both internal, external and those marked private or otherwise can be accessed by the IT Manager and / or Headteacher and it is agreed and accepted that the excessive use of the e-mail system for private e-mails is misconduct. You accept that such monitoring is necessary in order to prevent discrimination or harassment of any sort, taking place electronically within the organisation, as well as to enable the school to retain quality control.
➢ The forwarding of offensive, or pornographic e-mails is accepted as gross misconduct and may result in disciplinary action.
➢ I shall abide by the Computers and Data protection policy in the Staff Handbook at all times, and my use of the Company e-mail facility is subject to agreement to abide by such rules as are in force from time to time.
➢ I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
➢ I will not install any hardware of software without permission.
➢ I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
➢ Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
➢ I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
➢ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
➢ I will respect copyright and intellectual property rights.
➢ I will ensure that my online activity, in school will not bring my professional role into disrepute.
➢ I will report immediately to the ICT Coordinator damage or loss of any school ICT equipment.
➢ I will only access the internet for personal use prior to 08:00 & post 17:00 Monday - Friday. Such usage will be restricted to appropriate forums.
➢ I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature
I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …………………….…………… Date ……………………

Full Name …………………………………......................................(printed)

Drax Community Primary School

KS1 Acceptable Usage Policy

You will:
- **Always follow the instructions of your teacher when using the computers.**
- **Take care of the school electronic equipment.**
- **Keep your username and password secret.**
- **Always tell your teacher or a member of staff if you see, hear or read anything which makes you feel uncomfortable when using the computer.**

You will not:
- **Send anyone a message which is not nice.**
- **Use bad language or bad words on the computer.**
- **Try and log in as someone else.**
- **Search for things other than what you have been asked to do in your lesson.**

Do not share:
- **Your name**
- **Home address**
- **Telephone numbers**
- **Any personal information about you or your family and friends.**

When you are finished using the computer you must close it down properly following the instructions of your teacher.

I agree to follow the rules set out in this policy. I know that if I break any of these rules my parent/carer may be told and my use of school ICT equipment may be monitored

Name _____

Date_____

Drax Community Primary School

Key Stage 2 Acceptable Usage Policy

This document has been developed to help you understand the rules of using computers in school. You should always follow the rules set out in this policy because these rules will help keep you and your classmates safe.

When using the school's ICT equipment and other information systems, I have understood and will comply with the following statements:

- I have read and know what the computer rules in this document mean to me.

- I will only go on the internet using my own username and password.

- I will make sure that my password for the internet is difficult to guess and I will not share my password with anybody else.

- If I think someone has guessed my password I will tell a teacher.

- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I see anything like this I will tell my teacher immediately.

- I will not try and get to any websites that the school has blocked access to.

- I will make sure I take care of any school-owned ICT equipment that I use in school or at home.

- I will only use memory sticks with permission from my teacher.

- I will not install any software on school computers.

- I will return any school-owned ICT equipment to the head-teacher or to my teacher when I have finished using it.

- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my safety.

- I will not damage any school-owned ICT equipment.

- I will not eat or drink while using school-owned ICT equipment.

Social Media

- I know that some websites and social networks have age restrictions and I should not use them unless I am old enough.

- I will not say nasty or hurtful things about any member of staff or pupil online.

- I will not give away any of my personal details (full name, age, date of birth, sex, address etc.) or the personal details of other users in school, over the internet. This includes photographs or video images of me, other pupils or members of staff.

- I will never arrange to meet anyone I have only met online unless a trusted adult is with me.

- If I see any hurtful comments about the school, staff or pupils I will report them to the Headteacher.

Managing Digital Content

- I will only use school-owned equipment to create pictures, video and sound. Pictures, video and sound will not be taken without asking permission first.

- I will not publish anything online, e.g. images or pictures, without asking my teacher.

Mobile phones and devices

Mobile phones may be brought into school if parents require children to have them, but must be signed into the school office each day and collected at the end of the school day. Where possible the children should not bring a mobile phone to school.

- I will only use mobile phones and mobile devices (e.g. Nintendo DS) when my teacher tells me I can.

- I will not take pictures in school on my mobile phone or mobile device.

Agreement

- I agree to follow the rules set out in this policy. I know that if I break any of these rules my parent/carer will be told and my use of ICT equipment will be monitored.

Signed: _____

Drax Community Primary School

Pupil Acceptable Use Agreement - Parents

As part of pupils' curriculum enhancement and the development of ICT skills, Drax Community Primary School provides supervised access to the Internet including e-mail.

Although there are concerns about pupils having access to undesirable materials, we are taking positive steps to deal with this risk in school. Our school Internet access provider operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The school will not be liable under any circumstances for any damages arising from your child's use of the Internet facilities.

A copy of the school's E-Safety Policy is available for your inspection.

Should you wish to discuss any aspects of Internet use, please telephone to arrange an appointment.

PERMISSION FOR INTERNET ACCESS

I give permission for access to the Internet on the terms set out above.

Name of Child: _____

Signed: _____

Print name: _____

Date _____

E-Safety Policy Appendix 4

TEACHER TIPS FOR USING FACEBOOK

Here are some suggested guidelines for using Facebook safely:

 Ensure that all your privacy settings are set to 'Friends Only'. Go to your Account Settings and make sure that the Custom Settings are highlighted and that these show that status, photos and posts are set to 'Friends Only'.

 Consider what information you have on your info page and your profile picture. Including brief information and an unidentifiable picture, e.g. sunset, will assist in making your profile indistinctive.

 If you have professional and social 'friends' on Facebook, using the group list feature will ensure that you can distinguish what type of information you send to particular groups. Make sure that you do not accept pupils (even those that have recently left the school), parent or carers as 'friends'.

 Ensure that you do not bring your professional status and educational institute into disrepute. Make sure that you consider what you post about colleagues, pupils or parents. Taking charge of your digital reputation is important, as unprofessional posts or images will lead to disciplinary action and possible failure to gain employment in the future.

 Be careful what photographs you include on your profile, including photographs taken by others in which you are 'tagged'. Once these are uploaded, they are very difficult to remove and, using image editing software, they can be altered and merged with other more distasteful images. Use the 'untag' option to maintain privacy.

 Be aware of any spam or potential virus risks sent via rogue posts. It is advisable to check with anti-virus firms if you get any suspicious requests or posts.

 If you are alerted to any negative or unscrupulous information about yourself, colleagues or your school on Facebook, inform the Headteacher. Further advice to help with cyberbullying incidents etc., can be gained from a professional association such as your Trade Union.