Ferham Primary School

E-Safety Policy

September 2017

Date agreed by Governors: Delegated to the Headteacher

Review date: September 2018

The e-Safety Policy will be reviewed annually.

Why is Internet Use Important?

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 information and administration systems.

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 schools have 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 to take care of their own safety and security.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- exchange of curriculum and administration data with the Local Authority and DFE; access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

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

Authorised Internet Access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Local Authority helpdesk via the e-safety coordinator or network manager.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Pupils may only use approved e-mail accounts on the school system.
- 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.
- Whole class or group e-mail addresses should be used in school
- Access in school to external personal e-mail accounts are blocked.
- 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.
- Staff may send pupils e-mails via approved school email accounts, as this can be monitored by the e-safety coordinators. This should be within school hours and only be about school related work.

Social Networking

- School will block access to social networking sites and newsgroups unless a specific use is approved.
- Pupils will be advised about the rules of using social networking sites and we aim to educate children about the legal implications of improper use.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils should be advised not to place personal photos on any social network space.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.
- Staff are advised to use security settings within their social networking site to restrict information to only known friends. Staff can see the e-safety coordinator for help with this.
- It is not appropriate for staff to share work-related information whether written or pictorial via a social networking site.
- Under no circumstance should comments be made about other staff, pupils, parents/carers or school procedures on the Internet. Staff members should respect the privacy and the feelings of others. This could be deemed a disciplinary offence.
- Staff should not be friends with parents, carers or pupils on social networking sites. In situations where staff are friends with parents in a social capacity, it may be necessary for separate accounts to be held.
- If a member of staff believes something has been written which gives rise to concerns within this, or any other policy this must be discussed with the e-safety coordinator and a member of the Senior Leadership team.
- If a message or 'friend request' is received by a member of staff from a parent, carer or pupil, staff should ignore any messages and reject the request. Under no circumstances should staff reply as this can result in online information becoming available to others. Staff should inform the school e-safety coordinator about any messages or friends requests received from parents, carers or pupils.

Filtering

The school will work in partnership with the Local Authority, Internet Service Provider to ensure filtering systems are as effective as possible. Pupils will be taught how to block any sites they come across which are unacceptable e.g. CEOP.

Video Conferencing

- Video conferencing will always be done through an approved provider and will always be fully supervised in school.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile Phones

- Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Our school recommends that mobile phones are not brought into school unless the parental agreement is signed. These will then be stored securely in the school safe.

Publishing Pupils' Images and Work

- Photographs 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 Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

Protecting Personal Data

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

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 Rotherham Metropolitan Council can accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of 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 e-safety coordinator and a member of the school SLT.
- 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.
- All pupils and their parent/carer will be provided with a safe computer use agreement.

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.
- Staff will have read and signed the Staff Systems Code of Conduct.

Parents

Parents' attention will be drawn to the School e-Safety Policy in newsletters and the school brochure. They will have been asked to read our safe internet use rules and sign the agreement.

Staff, student and governors information systems code of conduct / Acceptable use policy

To ensure that all adults in our schools are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. We ask that all adults working in school consult the school's e-safety/Acceptable Use Policy for further information and clarification.

- The information systems (laptops, computers, web cameras etc) 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 will always be compatible with my professional role.

- I understand that school information systems may not be used for private purposes, without specific permission from a member of the federation leadership team. This includes the use of personal networking sites (Facebook, Friends Reunited, MySpace etc) and sites used for personal profit e.g. Ebay.

- I understand that I should use care and discretion when using any information systems (blogs, twitter etc.) or online communities (Facebook, MySpace etc.) so that my actions do not reflect badly upon myself or the school.

- I understand that it is not acceptable in my professional role to be 'friends' with pupils, parents or carers on a social networking site. If I am in the situation where I am friends with parents in a social capacity, it may be necessary for separate accounts to be held.

- I understand that it is unacceptable for me to communicate with pupils and their families through online communities, messaging services and social networking sites. I will report any pupils or parents requesting me as a 'friend' online or sending me messages to the e-safety coordinator.

- 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 not install any software or hardware to any school computer or laptop 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 Lead. This includes reporting any inappropriate websites, images or sounds which have made it through the schools firewall and filtering systems. I will also report any allegations or evidence of cyber-bullying to the safe guarding team.

- I will ensure that any electronic communications with pupils are compatible with my professional role. This will be through the agreed hours as outlined in the e-safety policy and will always be school-work related.

- I will remember to conduct myself online as I would do in the 'real' world in my professional capacity.

- 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. I will help educate my pupils about the effects and consequences of cyber-bullying and teach them ways of avoiding and dealing with this.

- If at any time I have concerns/worries about the e-safety of myself or pupils within school I will consult with the safe guarding team.

- I understand that failure to follow the school Acceptable Use and e-safety Policy may result in disciplinary action being taken against me by the school, governing body or the local authority.

- School insurance cover provides for the standard risks but excludes theft when left inappropriately unattended. This means that at the end of the school day laptops should be **locked** away and when away from school premises they should **never be left unattended.**

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 where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

If you have a laptop/computer equipment from school enter make and serial number below:

Make of computer:_____.

Serial number of computer:_____.

Make of camera:_____.

Serial number of camera:_____.

I have read the above and agree to the terms and conditions outlined:

Name:_____.

Signed:_____.Date:_____.

Ferham Primary Pupil E-Safety Agreement

This agreement should be read through with your parent(s)/carers. It informs you about Internet and Email Access in school.

- At Ferham Primary School we expect you to take responsibility for your own behaviour on the Internet, just as you do anywhere else in school.
- You will not deliberately seek out offensive materials. Should you encounter such material accidentally you are expected to report it immediately to a teacher or responsible adult.
- You must not use any rude or offensive language in your emails and contact only people you know or who have been approved by the teacher.
- You must ask permission from a teacher before accessing the Internet.
- You must not access other people's files unless permission has been given.
- The Computer should only be used for schoolwork and homework unless permission has been granted otherwise.
- You must not download any files to the computer from the Internet. This includes "Add-ons" such as Google taskbar.
- You must not bring in programs on disc, CD-ROM or USB memory card from home for use in school. This is both for legal and security reasons. If memory sticks are used, it is only when a member of staff has run a virus check and seen that the content of the files is appropriate to what the child is doing.

- You must not give out personal information such as phone numbers and addresses and you must not **under any circumstances** arrange to meet people over the Internet.
- Sometimes your work will be published electronically online. No photographs or full names will be given without permission from your parents/carers.
- We ask that you abide by online rules of conduct e.g. not have a FaceBook profile before the legal age of 13.
- You must not attempt to contact or add members of school staff, teaching students or volunteers through social networking websites or online contact programs e.g. MSN.
- You must never say or do anything online to upset or hurt anyone else. This can be seen as cyber-bullying and will be dealt with seriously.
- If you are worried about anything online, you must always report it to a responsible adult.

If you choose not to follow these rules you will be warned and may have your access to the Internet and Email account removed. If the incident is serious (e.g. cyber-bullying), the school has a legal responsibility to report this to CEOP (Child exploitation and online protection centre) and the local police.

Parents/Carers please read the above letter with your child and discuss being 'Cyber safe'.
If you have any queries or do not wish your child to access the internet or email within school, please speak to your child's class teacher.