# Wrenthorpe Primary School
# E- Safety Policy

January 2016

***Nominated E Safety Coordinators***: Leanne Staves (Computing Leader)
Jane Coyle (Headteacher)

## Writing and reviewing the E-safety policy

Our e-Safety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors.

The e-Safety Policy and its implementation will be reviewed annually.

## Teaching and learning

***Why Internet use is important*** - The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and learners.

***Internet use will enhance learning*** - The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of learners. Learners will be taught what is and is not acceptable Internet use and given clear guidance. This includes the SMART rules and regular e-safety training. Learners will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

***Learners will be taught how to evaluate Internet content*** - The school will ensure that the use of Internet derived materials by staff and learners complies with copyright law. Learners should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

***Physical safety*** **–** The following considerations are made when using technology:

- All electrical equipment in the school is tested annually to ensure that it is safe to use.
- Pupils are taught about the dangers of electricity as part of the science and PSHE curriculum.
- Health and safety guidance states that it is not healthy to sit at a computer for too long without breaks. Pupils are taught correct posture for sitting at a computer and that sitting for too long at a computer can be unhealthy.

- Computers and other ICT equipment can be easily damaged. Pupils are taught the correct way to use ICT equipment.

# Managing Internet Access

***Information system security*** – The following considerations are made to ensure the school network is safe:

- School ICT systems capacity and security will be reviewed regularly, with guidance from ICT4C.
- Virus protection will be updated regularly, with guidance from ICT4C.
- Security strategies will be discussed with ICT4C.
- All school computers require log-ins to gain access to the internet and network resources. Log-in and password information will not be shared.
- The access code for the school network will not be shared unless required for technical reasons, or for outside agencies to access required documents / sites.

***E-mail*** **–** In order to ensure our school email system remains a safe and secure place to exchange information, the following rules apply:

- Learners and staff may only use approved e-mail accounts on the school system.
- Learners must immediately tell a teacher if they receive offensive e-mail.
- Learners must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation 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.
- Any emails containing sensitive data / information will be zipped in order to protect the content. The passwords to access these files will not be sent in emails.

***Published content, the school website and blog***

- The contact details on the website and blog should be the school address, email address and telephone number. Staff or learners' personal information will not be published, other than details approved for the blog by parents/carers.
- The nominated website and blog leaders will take overall editorial responsibility and ensure that content is accurate and appropriate. This includes checking for parental permission for photographs and videos.
- Class Teachers will take responsibility for editing and updating their own sections (where relevant) on the website and blog, taking advice from the website and blog leaders.
- Learners' full names will not be used anywhere on the website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs or videos of learners are published on the school website and blog.

***Social networking and personal publishing***

- The school will block/filter access to social networking sites for learners.
- Social networking sites identified as a useful CPD/Information resource e.g. Twitter or Facebook will be made available to school staff, who must have completed E safety training and signed the Acceptable Usage Policy (AUP).
- Learners will be educated about the use and potential dangers of using social networking sites such as Facebook.

***Cyber bullying -*** Cyber-bullying is an aggressive intentional act carried out by an individual or group using electronic media repeatedly over time against a victim who cannot defend him or herself. Seven categories of cyber-bullying have been identified:

- Text messaging: sending picture or video-clips;
- Phone calling;
- E-mail messaging;
- Defamatory blogs;
- Personal websites;
- Personal space;
- On-line personal polling sites;

Bullying of any kind is not tolerated in the school. Any incidents reported will be logged, investigated and dealt with in line with the schools behaviour policy.

***Managing filtering -*** The school will work with ICT4C and the broadband provider to ensure systems to protect learners are reviewed and improved. If staff or learners discover an unsuitable site, it must be reported to the ICT coordinator. The ICT coordinator, along with ICT4C, will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Designated staff will have access to be able to change filtering options to ensure the safe and acceptable use of the internet within school.

***Managing emerging and mobile 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 will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff should not send text messages, emails or messages through social media sites to parents to discuss the school, the learners or any school business unless authorised by the Head Teacher.
- Learners will be educated in the appropriate use of emerging and mobile technologies, and what to do should they become aware of, or become victim of, inappropriate use.

***Ipad usage***

- E-mail, calendar and contacts cannot be accessed on the Ipads.
- The IPads must be initialised using a dedicated secure PC on the education network and have Apple’s firmware installed. A dedicated PC should be used to

remove the opportunity of someone plugging in their personal IPhone or IPad which may carry an application which could put a virus on the network.

- The IPads should be regularly updated using the dedicated PC, this is important in keeping the firmware up to date to fill gaps within the security measures.
- The IPads can be initialised, updated and restored by synchronising the IPad with the relevant software on the dedicated PC.
- Sensitive data should not be stored on the IPad.
- Any applications / information added to the iPads by staff at home must be removed before synchronising with the dedicated PC.
- Sharing work between iPad and the school network will be allowed with the introduction of a cloud-based portal.

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

# Policy Decisions

***Authorising Internet access***

- All staff must read and sign the 'Acceptable Usage Policy / E-behaviour agreement' before using any school ICT resource.
- The school will keep a record of all staff and learners who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- Access to the Internet for learners will be supervised by an adult.

***Assessing risks***

- The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer.
- Neither the school nor Wakefield LEA can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision annually to establish if the E-safety policy is adequate and that its implementation is effective.

***Handling E-safety complaints***

- Complaints of Internet misuse will be dealt with by a senior member of staff and/or the E safety coordinator.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Learners and parents will be informed of the complaints procedure.

# Communications Policy

***Introducing the E-safety policy to learners***

- E-safety rules will be posted in all networked rooms and discussed with the learners at the start of each year.
- Learners will be informed that network and Internet use will be monitored.
- Learners will be reminded of e-safety rules throughout the year as appropriate, and in a cross-curricular way.

***Staff and the E-Safety policy***

- 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.

***Enlisting parents' support***

- Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school blog.
- E-safety advice for parents will be offered through leaflets and letters home, E-safety 'open evenings' and having a range of materials available at parents evenings.

# Reporting procedure

- Any breach / safety issue will be reported as soon as it comes to light.
- Any incident immediately relating to / posing a risk to child protection will be referred immediately to the Head Teacher, who will investigate this accordingly.
- Any concern regarding the conduct of a member of staff, or breach of school ICT systems rules by a learner will be referred immediately to the ICT / E-safety coordinator to be dealt with accordingly.

# Failure to comply

Failure to comply in any way with this policy will be considered a serious risk to health & safety and all incidents of non-compliance will be dealt with accordingly.

To be reviewed January 2017.

January 2016
Jane Coyle / Leanne Staves