Wickersley Northfield Primary

Part of White Woods Primary Academy Trust

E-Safety Policy

August 2016

Introduction

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The main aims of our e-safety police are:

To set out the key principles expected of all members of the school community at Wickersley Northfield Primary School (WNP) with respect to the use of ICT-based technologies.

To safeguard and protect the children and staff of WNP.

Scope

Statements

This policy applies to the whole school community including WNP's Senior Leadership Team, school board of governors, all staff employed directly or indirectly by the school and all pupils.

WNP's senior leadership team and school board of governors will ensure that any relevant or new legislation that may impact upon the provision for e-Safety within school will be reflected within this policy.

School e-safety policy

Writing and reviewing the e-safety policy

- The e-Safety Policy is part of the School Development Plan and relates to other policies including those for Computing and for child protection.
- The school's e-Safety Coordinator is also the ICT Coordinator (Vicky Harrison). She works in close co-operation with the head teacher and business manager.
- The head and business manager are the Designated Child Protection Officers.
- Our e-Safety Policy has been written by the school. It has been agreed by the
- Staff and governors.
- The e-Safety Policy will be reviewed January 2017 (The school e-Safety coordinator will be responsible for document ownership, review and updates)

Communication Policy

We believe that e-Safety is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Roles & Responsibilities

Senior Leadership Team

- The head teacher is ultimately responsible for e-Safety provision for all members of the school community, though the day-to-day responsibility for e-Safety will be delegated to the e-Safety coordinator.

Responsibilities of the e-Safety Coordinator

- To promote an awareness and commitment to e-Safety throughout the school
- To be the first point of contact in school on all e-Safety matters
- To take day-to-day responsibility for e-Safety within school and to have a leading role in establishing and reviewing the school e-Safety policies and procedures
- To ensure that all members of staff receive an appropriate level of training in e-Safety issues
- To ensure that e-Safety education is embedded across the curriculum
- To ensure that e-Safety is promoted to parents and carers
- To ensure that an e-Safety incident log is kept up to date

Responsibilities of teachers and support staff

- To read, understand and help promote the school's e-Safety policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To model safe and responsible behaviors' in their own use of technology
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
- To maintain a professional level of conduct in personal use of technology at all times

Responsibilities of technical staff

- To read, understand, contribute to and help promote the school's e-Safety policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Policy
- To report any e-Safety related issues that come to your attention to the e-Safety coordinator.
- To support the school in providing a safe technical infrastructure to support learning and teaching
- To ensure that provision exists for misuse detection and malicious attack
- To take responsibility for the security of the school ICT system

- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster

Responsibilities of pupils

- Pupils will ensure that all equipment is used in a respectable and safe manner.
- All breakages or damage will be reported to a member of staff.
- E-safety learning will be applied when using all equipment.

Responsibilities of parents and carers

- To help and support the school in promoting e-Safety

Responsibilities of the governing body

- To read, understand, contribute to and help promote the school's e-Safety policies and guidance
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils

Responsibilities of other external groups

- The school will liaise with local organisations to establish a common approach to e-Safety and the safe use of technologies.

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 pupils. 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 pupils. This is supplied by YGFL.
- 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 the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

- Pupils will be taught how to evaluate Internet content.

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the school ICT Coordinator or business manager.
- Staff should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Digital Content

Written permission from parents or carers will be obtained for the following locations before photographs of pupils are published. This will be done as part of the home-school agreement on entry to the school.

On the school website
In the school prospectus and other printed promotional material, e.g. newspapers
In display material that may be used around the school
In display material that may be used off site
Recorded or transmitted on a video or via webcam in an educational conference

- Parents and carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.
- We will remind pupils of safe and responsible behaviors' when creating, using and storing digital images, video and sound.
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

Storage of images

- *Any* images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment.
- No personal cameras or phones are to be used to take pictures of children.
- No images of children are to be stored on memory sticks.

Managing Internet Access

Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly. (Technician's responsibility)
- The school uses rgfl broadband with its firewall and filters.

E-mail

- Pupils may only use approved e-mail accounts on the school system. Children are not allowed access to personal e-mail accounts or chat rooms whilst in school.
- 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.
- 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.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Staff email addresses are not to be given out to parents/ children.

Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils. (YouTube, instagram, facebook all have a legal age of 13)

Managing filtering

- The school will work in partnership with the service provider to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety coordinator or business manager.
- Senior staff will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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 (staff and pupils) will not be used during lessons or formal school time. Children are to hand in mobile phones to reception upon arrival.

- The sending of abusive or inappropriate text messages is forbidden.

- Staff have access to a school phone where contact with parents/pupils is required.

Protecting personal data

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

Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff, including Teaching Assistants and Supply Teachers must read and sign the acceptable ICT Acceptable User Policy (AUP) before using any school ICT resource.
- At EYFS/Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents and pupils will be asked to sign and return a consent form agreeing to comply with the school's Acceptable Use Policy. (Home/school agreement)

.

Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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. The school can accept liability for the material accessed, or any consequences of Internet access.
- The head teacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

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 head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Staff Training

- Our staff receives regular information and training on e-Safety issues in the form of annual training.

- As part of the induction process all new staff receive information and guidance on the e-Safety policy and the school's Acceptable Use Policies.

Signed :___________________________________ position ____________________

Signed : __________________________________ E-Safety Coordinator

Signed: __________________________________ Headteacher

Signed: __________________________________ Chair of Governors

Date: ____/____/_____