Alderman Pounder Infant and Nursery School

Online Safety Policy

Document Owner: Head Teacher

Issue Date: Autumn 2017

Version: 1.4

Review frequency: Annual

REVISION HISTORY

Version	Revision Date	Next review due	Summary of Changes (and author)
1.0	Autumn 2014	Autumn 2015	Reviewed and agreed at Resources 16.10.14
1.1	Autumn 2015	Autumn 2016	Reviewed. Staff details updated. Prevent duty
1.2	Summer 2016	Autumn 2016	Prevent Duty statement
1.3	Autumn 2016	Autumn 2017	No Change. Agreed 03.10.16 at C&P
1.4	Autumn 2017	Autumn 2018	Policy name change: E-Safety to Online Safety Name change from Mrs Shelton to Miss Hemsley

Policy Development

The Online Safety policy relates to other policies including those for Understanding the World, Anti-bullying and Safeguarding children.

- ✓ Our policy has been written with full consultation from staff in school, parents/carers, governors and young people.
- ✓ It has been agreed by senior managers and approved by governors.
- ✓ The policy and its implementation will be reviewed annually.
- ✓ It is available to read or download on our school website or as a hard copy from the school office.

Roles and responsibilities

- The school's Designated Safeguarding Lead will be responsible for Online Safety
- Our coordinator is: Miss J Hemsley (Head Teacher)

Teaching and Learning

Why internet and digital communications are important

- The purpose of any technology in school is to raise educational standards, to promote achievement, to support the professional work of staff and to enhance the school's management functions.
- The school has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for staff.
- Pupils will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- They will be encouraged to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be shown how to publish and present information appropriately to a wider audience.
- Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for use. These are also important transferable skills for their life out of school, including using mobile phones and other mobile devices.
- Pupils will be taught how to report unpleasant internet content including Cyberbullying or unwanted contact. This will include using the Hector Protector function.

- Issues such as Cyberbullying and online safety will be built into the curriculum to encourage self-efficacy and resilience. Some children who have had problems, or who have additional needs, may need additional support.

Managing Internet Access

Information security system

- The school ICT system security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies may be discussed with the Local Authority.

E-mail

- Staff may only use approved e-mail accounts on the school system.
- Pupils do not have access to email in school.
- All incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Published content and the school website

- The contact details on the school's website should be the school address. No staff or pupil's personal details will be published.
- The Deputy Head Teacher will have overall editorial responsibility to ensure that our website content is accurate and appropriate.

Publishing pupils' images and work

- Group photographs will be used rather than full-face photos of individual children.
- Pupil's full names will be avoided on the website.
- Written permission will be obtained from parents and carers before any photographs are published on the school website.
- Parents should be clearly informed of the school policy on image taking and publishing.

Social networking

- The school will not promote the use of social networking.
- The school will strongly discourage parents from allowing their children on social networking sites as all children are under the age of 13.
- The school's home/school agreement will discourage parents from using social networking as a way of voicing their opinion about the school or the staff.

Managing filtering

- The school will work with the county council to ensure systems to protect pupils are reviewed and improved.
- Any unsuitable on-line material should be reported to the Head Teacher.
- Regular checks will be made to ensure the filtering methods are appropriate, effective and reasonable.
- A log will be kept and used to identify patterns and behaviours and therefore inform policy and educational interventions.

Managing video conferencing

- Videoconferencing will be appropriately supervised for the pupils' age.
- Videoconferencing will use the educational broadband network to ensure quality of service and security.

Managing emerging technologies

- The school will examine emerging technologies for their educational benefit and carry out a risk assessment before use in school.
- Staff's mobile phones will not be used in lessons.
- Staff will use a school phone where contact with pupils and their families are required.

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 'staff code of conduct' and Acceptable Use policy before using any school ICT resource.
- At Key Stage 1, access to the internet will be by adult demonstration with directly supervised access to specific on-line materials.
- 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 it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school will monitor ICT use to establish if the e-safety policy is appropriate and effective.

Handling online safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Complaints of misuse by staff will be referred to the Head Teacher.
- Any complaints of a child protection nature must be dealt with in accordance to child protection procedures

Community use of the internet

- All use of the school internet connection by community and other organisations shall be in accordance with the online safety policy.

Communicating the Policy

Pupils

- Appropriate elements of the online safety policy will be shared with pupils.
- Online safety rules will be posted in all classrooms.
- Age appropriate curriculum opportunities will be used to ensure all pupils gain an awareness of online safety. These will be addressed on a regular basis and modified as newer risks are identified.

Staff

- All staff will be given a copy of the online safety policy and required to sign to acknowledge that they have read and understood the policy and agree to work within the guidelines.
- Staff should be aware that the system is monitored and that professional standards are expected.
- Staff monitoring the system will be supervised by senior management and have a clear procedure for reporting.
- Staff will ensure that children are safe from unsuitable materials including extremist and terrorist content.

Parents

- Parents will be notified of the online safety policy in newsletters, the school prospectus and website.
- All parents will be asked to sign the home/school agreement when they register their children.
- Parents will be offered online safety training to encourage them to support and encourage positive online activities with their children and help them to use the internet safely.

Prevent duty

- Every member of staff recognises that safeguarding against radicalisation and extremism is no different to safeguarding against any other vulnerability in today's society.
- We protect children from the risk of radicalisation, for example by using filters on the internet to make sure they can't access extremist and terrorist material, or by vetting visitors who come into school to work with pupils.
- Our Safeguarding, Prevent Duty and Online Safety policies set out our beliefs, strategies and procedures to protect vulnerable individuals from being radicalised or exposed to extremist views, by identifying who they are and promptly providing them with support.