FOREFIELD COMMUNITY INFANT & NURSERY SCHOOL

POLICY FOR E-SAFETY

January 2016

FOREFIELD COMMUNITY INFANT & NURSERY SCHOOL E-SAFETY POLICY

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Our E-Safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings. The policy is organised in 4 main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection.

Policies and Practices

Forefield Community Infant & Nursery School ensure that all our children will learn in an environment where security measures are balanced appropriately with the need to learn effectively. We provide a diverse, balanced and relevant approach to the use of technology and encourage our children to maximise the benefits and opportunities that technology has to offer. Our children are taught in an age-appropriate way, to recognise the risks associated with technology and how to deal with them, both within and outside the school environment by equipping them with the skills and knowledge to use technology appropriately and responsibly.

Our E-Safety Champion is Mrs Bev Roberts whose role it is, to:

- develop, maintain and review the schools E-Safety Policy and Acceptable Use Policies
- in conjunction with the Headteacher and Governing Body, ensure the policy is implemented & complied with
- ensure all staff are aware of reporting procedures should an E-Safety incident occur
- ensure the CPOMS E-Safety Incident Log is appropriately maintained and regularly reviewed
- keep up-to-date with E-Safety issues and arrange E-Safety advice/training as appropriate.

This E-Safety policy should be read in conjunction with the Computing, Social Media, and Image Policy and the following related policies and documents. Each of these documents details specific E-Safety aspects including specific benefits and associated risks relevant to the policy within an E-Safety context and the appropriate management of them:

- Anti-bullying Policy
- Behaviour & Discipline
- Safeguarding Policy
- Foundation Stage Policy
- Staff Handbook

In addition, an Acceptable Use Policy is issued to all staff, pupils, parents/carers, visitors and school community users to ensure that all users of technology within school will be responsible and stay safe.

Infrastructure and Technology

The filtering of internet content is an important means of preventing users accessing illegal or inappropriate material. A filtering system cannot, however, provide 100% guarantee that it will do so, as such pupils will be made aware of the importance of internet safety through the E-Safety Education Programme.

The school is subject to the Arvato global internet filtering and its policy as outlined in the Schools ICT Support SLA. This filtering policy is reviewed and improved by the provider.

[The responsibility for the management of the schools filtering policy will be held by the E-Safety Champion. They will manage the school filtering, and in line with this policy, will record any change to the global policy and any breaches of the system that may occur].

If staff or pupils come across unsuitable content online, they must report this to the Computing/E-Safety Coordinator straight away. A report will then be made to the Internet Service Provider via the IT Coordinator referring to the URL (address) of the unsuitable site and its content. This will be recorded in the E-Safety Log. The E-Safety Champion in conjunction with the Headteacher will ensure regular checks are made to ensure the filtering is appropriate, effective and reasonable for our schools. Any material that the school believes is illegal must be referred to CEOP via the reporting icon installed on the desk top of all computers in the ICT Zone.

Managing Information Services

The school ICT system will be reviewed regularly with regard to security. Virus protection will be installed and updated regularly in conjunction with the school's chosen Technical Support Provider. Security strategies will be discussed and changes made as deemed appropriate after discussion with the Computing Co-ordinator/Headteacher. The use of data storage facilities by pupils within school is prohibited to protect against virus transfer. Files held on the school's network will be regularly checked.

Pupils do not have school-based email accounts. Emails written by staff to external organisations should be written carefully and professionally, in the same way as a letter written on school headed paper and be sent from school email addresses only. Emails to parents should be sent through the school admin email address.

The point of contact on the website will be the school address, school e-mail and telephone number. Staff or pupils' personal information will not be published. The Headteacher will take overall editorial responsibility and ensure content is accurate and appropriate on all pages directly related to the day-today workings of the school. At present editorial responsibility for all other areas of the website is the responsibility of Bev Roberts. The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Images which include pupils will be carefully selected and only those children whose written parental permission (obtained on entry to school) has been sought will be identifiable. Class teachers will be responsible for ensuring photographs selected show only these pupil (See AUP). Pupils' full names will not be used on the website when associated with photographs, or in any way which may be to the detriment of pupils. Pupil photographs will immediately be removed from the school website upon request by parents, or other appropriate request.

Education and Training

This school believes in equipping pupils with the appropriate skills and abilities to recognise the risks and how to deal with them. E-safety is embedded into the computing curriculum and is taught as part of each module through the Rising Stars computing scheme used in Key Stage 1. In addition an E-Safety education programme is delivered each year using the following age specific resources.

Nursery & Reception - SMART rules for internet safety delivered through the Adventures of Smartie the Penguin on Kidsmart website In the Foundation Stage, pupils are taught to not give any personal information on the internet. They are told to tell a teacher or parent if anything they see on the internet makes them feel uncomfortable. At Forefield, we do not expect children of this age to be unsupervised whilst using the internet. Reception pupils take part in the school "Internet Safety Week" using age appropriate CEOP resources.

Y1 and Y2 – SMART Rules for internet safety delivered through the CEOP education programmes, Hectors World in Y1 and Lee and Kim in Y2. Pupils begin to understand what personal information is and who you can share it with. Children begin to recognise the difference between real and imaginary online experiences. They are taught to keep their passwords private and only access the internet under adult supervision in school. They are taught to always make sure that an adult knows what they are doing online. Four key messages taught at Key Stage 1:

- People you don't know are strangers. They're not always who they say they are.
- Be nice to others on the internet, like you would on the playground.
- Keep your personal information private.
- If you ever get that 'uh-oh' feeling, you should tell a grown-up you trust.

Staff will undertake regular E-Safety training and receive regular updates and be made aware of changes or trends in E-Safety issues. Staff will all accept and sign Acceptable Use Policy before using any school devices or technology.

Parents and Governors are offered E-Safety awareness sessions and specific guidance will be issued in the form of newsletters, leaflets and Digital Parenting magazines. Information, updates and links to websites will also be available on the school website.

Parents will be informed of and asked to sign the Acceptable Use Policy.

Acceptable Use of Personal Equipment

- **Use Social networking sites**

Use of social networking sites for personal use, such as Facebook from a school computer whilst on school premises is not permitted. Social networking sites can be accessed on personal handheld devices by staff & volunteers at break times only. Access to social media for personal use whilst using the school Wifi is not permitted. Should staff/volunteers use the school Wifi system at any point, their personal device becomes subject to school property E-Safety checks for appropriate use (See AUP appendix/amendment).

- **Use of Mobile Phones and other personal mobile devices.**

Staff/volunteers should not use their own mobile phones or devices to take photos of children in school or on school visits. Mobile phones and other personal mobile devices can be accessed at break times only in areas away from children.

- **Use of Cameras/IPad Images of pupils and/ or staff must only be stored on computers / drivers owned by the school.**

Images must be taken using school owned devices & SD cards which must be kept securely in school at all times. Images will not be distributed outside the school network (e.g. Website / local press) without the permission of the parent/ carer, member of staff or Headteacher. Images taken on any other devices will be shared with the E-Safety Champion or Headteacher, and dealt with in accordance with the image policy.

- **Email**

Emailing is one of the primary ways we communicate with each other, however the system should be used responsibly and staff should always act in a professional manner when using the system. Members of staff should always use their school email addresses for any email correspondence linked to school, children or staff. (See Acceptable Use Policy). Members of staff should not feel obliged to reply to any emails sent to them in the evenings or at weekends and equally staff should not expect a reply from colleagues outside school hours.

Standards and Inspection

To ensure E-Safety standards are maintained;

- all E-Safety incidents will be recorded on an incident log on CPOMS
- the incident log will be monitored and reviewed termly by the E-Safety Champion in conjunction with the Headteacher to identify possible recurring patterns, additional education or training needs and required amendments to existing policies and practices.
- findings of this review will be reported back to governors.
- Any new technology introduced within school will be assessed to ensure that is of educational benefit and that any security risks posed can be appropriately managed before use in school is allowed.
- Mobile phone use is not permitted by children. Staff and visitors to school are advised during induction that use is not permitted in classrooms or around school with children in the building except in the main entrance /staffroom area.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- All staff and pupils will initially be granted Internet access. Parents will be asked to sign a written consent form giving permission for supervised access for pupils. Pupils will not be allowed to use

computers/tablets with Internet access unless they are directly supervised by a member of staff. SMART guidelines and visual reminders for Internet safety are visible around the school.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- The content of the E-Safety Policy and associated policies and practices will be reviewed annually to ensure appropriate reference to current E-Safety trends and new technologies.

Handling Complaints or Concerns

The school will deal with all incidents and offences using the procedures outlined below. Any incident or offence will be recorded using the attached E-Safety Incident Log on CPOMS. Both the outcomes and recorded incidents will be regularly monitored and audited on a termly basis by the E-Safety Champion in conjunction with the Headteacher. Responsibility for handling e-safety incidents is delegated to a member of the Senior Leadership Team, Bev Roberts. Parents and pupils will need to work in partnership with staff to resolve issues following the school's Complaint's Procedure. Under certain circumstances, external agencies may be contacted to establish the legal position and discuss strategies e.g. Education Welfare Service, Police. Sanctions available include:

- Interview by senior member of staff/class teacher
- Informing parents or carers
- Removal of internet or computer access for a period of time.

Any complaints about staff misuse must be referred to the Headteacher.

Communication of E-Safety Policy to Pupils

Pupils - An age appropriate E-safety training programme will be used to raise awareness of the importance of safe and responsible Internet use both at home and at school. Internet safety guidelines will be reinforced through posters prominently displayed near all computers in school. Pupils will be verbally reminded of school policy decisions e.g. only supervised access to the Internet, on a regular basis by all staff.

Staff – All staff will be given the school E-Safety Policy and its application and importance explained. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. The monitoring of the Internet is a sensitive matter and should only be operated under instruction from the Senior Leadership Team. Staff training in safe and responsible Internet use, and on the school E-Safety Policy will be provided as required.

Parents – Parents' attention will be drawn to the school's E-Safety policy in newsletters, leaflets and on the website. Internet issues will be handled sensitively to inform parents without undue alarm. A partnership approach with parents will be encouraged. This will include leaflets, booklets and workshops for safe internet use at home.

January 2016

Bev Roberts