Forefield Junior School

Online Safety Policy

November 2017

Review 2018

Mission Statement

*Forefield Junior School is a **P.R.O.U.D.** school built on **Passion** and **Respect**, where **Opportunities** can be seized by **Unique** and **Determined** learners.*

We are passionate about learning in an environment where everyone is empowered to be themselves and to flourish. We respect and value each and every individual and cherish their unique qualities to create a sense of belonging. We are determined to support personal, social and emotional development by encouraging self-belief and providing opportunities for everyone to express themselves and grow in confidence.

By celebrating their diverse contribution to the life of the school and the wider community, each person will be encouraged to build on their foundations, to instil a belief in everyone that they have limitless potential and are always capable of achieving their best - throughout their lives. As a family we share each other's successes and take pride in them.

We will consistently promote the highest of standards in every aspect of school life, provide a vibrant, stimulating curriculum in a safe and happy learning environment, to foster excellent attitudes and behaviour. The inspirational opportunities we provide will fuel a passion for learning and a sense of pride in all we do.

This is what makes us PROUD:

Passion, Respect, Opportunity, Unique, Determined.

1.1 Who will write and review the policy?

The e-Safety Policy is part of many different schools policies including the Computing/ICT Policy, Child Protection or Safeguarding Policy, Anti-Bullying and should relate to other policies including those for behaviour, for personal, social and health education (PSHE) and for citizenship.

1.2.1 Why is Internet use important?

Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

• 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 functions.

• Internet access is an entitlement for students who show a responsible and mature approach to its use.

1.2.2 How does Internet use benefit education?

Benefits of using the Internet in education include:

• access to worldwide educational resources including museums and art galleries;
• inclusion in the National Education Network which connects all UK schools;

• educational and cultural exchanges between pupils worldwide;
• vocational, social and leisure use in libraries, clubs and at home;
• 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 networks of schools, support services and professional associations;
• improved access to technical support including remote management of networks and
automatic system updates;
• exchange of curriculum and administration data with SMBC and DfE;
• access to learning wherever and whenever convenient.

1.2.3 How can Internet use enhance learning?

The school's Internet access will be designed to enhance and extend education.
Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
The school will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
• Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
• Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
• Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
• Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

1.2.4 How will pupils learn how to evaluate Internet content?

Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
Pupils will use age-appropriate tools to research Internet content.

1.3 Managing Information Systems

The security of the school information systems and users will be reviewed regularly. Virus protection will be updated regularly.

• Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
• Users must take responsibility for their network use.
• Workstations should be secured against user mistakes and deliberate actions.
• Servers must be located securely and physical access restricted.
• The server operating system must be secured and kept up to date.
• Virus protection for the whole network must be installed and current.
• Unapproved software will not be allowed in work areas or attached to email.
• Files held on the school's network will be regularly checked.

• The network manager will review system capacity regularly.
• The use of user logins and passwords to access the school network will be enforced.

1.3.2 How will email be managed?

Pupils may only use approved email accounts for school purposes. Pupils must immediately tell a designated member of staff if they receive offensive email. Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult. Whole-class or group email addresses will be used in primary schools for communication outside of the school.
Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.

- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.

1.3.3 How will published content be managed?

The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published. Email addresses will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT'.) The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate. The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

1.3.4 Can pupils' images or work be published?

Images or videos that include pupils will be selected carefully and will not provide material that could be reused. Pupils' full names will not be used anywhere on the website, particularly in association with photographs. Written permission from parents or carers will be obtained before images/videos of pupils are electronically published. Pupils' work can only be published with their permission or the parents. Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.

1.3.5 How will social networking, social media and personal publishing be managed?

The school will control access to social media and social networking sites.

Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc. Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible. Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

• All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
• Newsgroups will be blocked unless a specific use is approved.
• Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
• Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined.

1.3.6 How will filtering be managed?

The school's broadband access will include filtering appropriate to the age and maturity of pupils. The school will work with the appropriate bodies to ensure that filtering policy is continually reviewed. The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure. If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate. The School filtering system will block all sites on the Internet Watch Foundation (IWF) list. Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.

The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective. Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Merseyside Police or CEOP. The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

1.3.7 How will videoconferencing be managed?

All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer. Videoconferencing contact information will not be put on the school Website. The equipment must be secure and if necessary locked away when not in use. School videoconferencing equipment

will not be taken off school premises without permission. Responsibility for the use of the videoconferencing equipment outside school time will be established with care.

Pupils will ask permission from a teacher before making or answering a videoconference call. Videoconferencing will be supervised appropriately for the pupils' age and ability. Parents and carers consent should be obtained prior to children taking part in videoconferences.

• Only key administrators should be given access to videoconferencing administration areas or remote control pages.
• Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.
When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.
• Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
• If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
• Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

1.3.8 How are emerging technologies managed?

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school's policies.

1.3.9 How should personal data be protected?

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

1.4.1 How will Internet access be authorised?

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
• Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
• When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).
Pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

1.4.2 How will risks be assessed?

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor SMBC can accept liability for the material accessed, or any consequences resulting from Internet use.
The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
• The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Merseyside Police.
• Methods to identify, assess and minimise risks will be reviewed regularly.

1.4.3 How will the school respond to any incidents of concern?

• All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
• The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
• The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
• The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
• The school will inform parents/carers of any incidents of concerns as and when required.
• After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
• Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police.
• If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County e-Safety Officer.

1.4.4 How will e–Safety complaints be handled?

Complaints about Internet misuse will be dealt with under the School's complaints procedure. Any complaint about staff misuse will be referred to the head teacher. All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
• Pupils and parents will be informed of the complaints procedure.
• Parents and pupils will need to work in partnership with the school to resolve issues.

• All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting
concerns.
• Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguard Team to establish procedures for handling potentially illegal issues.
• Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
• All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

1.4.5 How is the Internet used across the community?

• The school will liaise with local organisations to establish a common approach to e–Safety.
• The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
• The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.

1.4.6 How will Cyberbullying be managed?

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour. There are clear procedures in place to support anyone in the school community affected by cyberbullying. All incidents of cyberbullying reported to the school will be recorded. There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.

• Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
• The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
• Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
• The bully will be asked to remove any material deemed to be inappropriate or offensive.
• A service provider may be contacted to remove content if the bully refuses or is unable to delete content.
• Internet access may be suspended at school for the user for a period of time.
• Parent/carers of pupils will be informed.
• The Police will be contacted if a criminal offence is suspected.

1.4.7 How will mobile phones and personal devices be managed?

The use of mobile phones and other personal devices by students and staff in school will be decided by the school. The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy. School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.
• Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
• Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets and swimming pools.
• If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
• Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
• Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

1.5 Communication Policy

1.5.1 How will the policy be introduced to pupils?

All users will be informed that network and Internet use will be monitored.
• Pupil instruction regarding responsible and safe use will precede Internet access.
• An e–Safety module will be included in the Computing programme covering both safe school and home use.
• e–Safety training will be part of the transition programme across the Key Stages and when moving between establishments.
• e-Safety rules will be posted around the school.
• School Council will create a child-friendly Acceptable Use Code of Conduct.
• Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

• Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

1.5.2 How will the policy be discussed with staff?

The e–Safety Policy will be formally provided to and discussed with all members of staff. To protect all staff and pupils, the school will develop an Acceptable Use Code of Conduct. Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
• Staff who manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
• The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
• All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

1.5.3 How will parents' support be enlisted?

Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.
• A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings and sports days.
• Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement.
• Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss it's implications with their children.
• Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.
• Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.