Fairisle Infant and Nursery School

E-Safety Policy

Date policy reviewed: February 2019

To be reviewed again: February 2021

Ratified by the Governing Body: 6.3.19

Signature: A Stephens

Fairisle Infant and Nursery School

E-Safety Policy

Every child has the right to reliable information from the media. This should be information that children understand. Governments must protect children from materials that could harm them. **Convention on the Rights of the Child Article 17**
Every child has the right to feel safe. **Convention on the Rights of the Child Article 19**

Our e-Safety Policy has been written by the school, Southampton City Councils e-safety and government guidance. It has been agreed by the leadership team and approved by the governors. This policy will be reviewed annually.
This policy applies to all people using school equipment. This includes teaching staff, administration staff, ancillary staff, site managers, students, pupils, parents and visitors. FINS will ensure that every person to whom this policy applies is aware of its contents.
The E-Safety policy is to be read in conjunction to other policies including Child Protection, Safeguarding, Computing, Data Protection Privacy Notice, Teaching and Learning policy, Behaviour policy, Acceptable use of the Internet Policy (2009), Anti-Bullying, Complaints Procedure and Mobile phone and camera policy.

Teaching and learning

Why the Internet and digital communications are important?
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 information and business administration systems. Access to the Internet is a necessary tool for staff and an entitlement for pupils to give them experience of developments in technology in the world around them.

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 the pupils. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for Internet use. Pupils will be taught how to evaluate Internet content and the school will ensure that the use of Internet derived materials by staff and pupils complies with the copyright law.
The computing curriculum (KS1 and EYFS) teaches children E-Safety. Children are taught the Lock it, Block it, Show it, Tell it slogan to support keeping themselves, others and their personal details safe online and what to do should they come across content that scares or upsets them. Pupils are constantly reminded of online safety across the curriculum where appropriate.
To support teaching and learning and to access the Computing and other curriculums, children in YR- Y2 are provided with access to Purple Mash (2Simple), our school's online learning platform. Children are provided with a username and password and are taught how to store these confidentially. With signed parental permission, pupils have the opportunity to access the learning platform at home. Teaching staff have access to view and monitor the accounts of pupils in their class.

Managing Internet Access

Information system security

- The school ICT system security will be reviewed regularly.
- Firewall and virus protection is provided by Southampton City Council for computers connected to the schools network. The school will ensure that the virus definition files are updated regularly on all school machines to maintain protection.
- Security strategies will be discussed with the Local Authority.
- Memory keys and external drives are not permitted to be used.

E-mail and on-line communication

- Pupils may only use approved e-mail accounts on the school system with the supervision of teaching staff.
- Pupils may send e-mail as part of planned lessons where whole-class or group e-mail addresses set up by the Computing subject leader or Technician will be used. Formal e-mails sent to an external organisation should be written carefully and authorised (by the Headteacher) before sending, in the same way as a letter written on school headed paper.
- Pupils will be taught the Lock it Block it Show it Tell it chant to teach them that:
  * they must immediately tell a teacher if they receive offensive e-mail
  * they must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail or on-line communication.
  * in-coming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Published content and the school web site

- Staff or pupil personal contact information will not be published. The contact details given online should be the school office.

Publishing pupils images and work

- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Recognisable photographs and pupils' full names will not be used anywhere on the school web site or other on-line space. Where photographs of children are used, signed parent/carer permission must be obtained before being published online.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Social networking and personal publishing

- Whilst the School does not wish to discourage staff from using such sites on the Internet in their personal time, it does expect certain standards of conduct to be observed in order to protect the School and its reputation, and also to protect staff from the dangers of inappropriate use.

  Accessing social networking sites in working time and/or from School ICT equipment is strictly forbidden, whether the equipment is used at home or at school.

Friends/Befriending:

One of the functions of social networks is the ability to "friend" others, creating a group of individuals who share personal news and /or interests. Staff must not initiate or accept

invitations to “friend” pupils, or pupil’s family members/friends. However, there may be exceptions e.g. family members where a pupil is related to a member of staff.

Staff who maintain social networking friendships, are required to adhere to the requirements below relating to content of interactions.

Content of interactions:

Staff are recommended to refrain from making reference on social networking sites to the School, its employees, pupils, and their families. If staff adhere to this recommendation then the personal content of an individual’s social networking memberships is unlikely to be of concern to the School.

An exception to the above would be content which details conduct outside of employment which affects the individual’s suitability to perform his/her work, makes him/her liable to be unacceptable to other staff or management, or is liable to damage the School’s reputation.

If employment at the School is referred to, then the information posted would need to comply with the conditions set out below.

- Any references made to the School, its employees, pupils and their families, should comply with the School’s policies on conduct/misconduct, equal opportunities, and bullying and harassment.

- Staff must not post information on a social networking site which is confidential to the School, its employees, its pupils or their families.

- Staff must not post entries on social networking sites which are derogatory, defamatory, discriminatory or offensive in any way, or which have the potential to bring the School into disrepute.

- Staff should not use the School logo on their own personal social networking accounts, and should not post any photographic images that include pupils.

- When posting any information onto a social networking site, staff are recommended to consider whether any entry they make puts their effectiveness to perform their normal duties at risk.

- If individuals feel aggrieved about some aspect of their work or employment, there are appropriate informal and formal avenues, internally within the School, which allow staff to raise and progress such matters. Social networks are not the appropriate forum to raise such matters. Employees should discuss any concerns with their head teacher/line manager in the first instance. Guidance is also available from HR/Payroll and trade unions.

Where staff use educational/professional networking sites as a professional resource, which are not available to the general public; it is acceptable to make reference to the school. The above conditions relating to content of postings/communications will still apply.

Security

Staff are advised to check their security profiles and privacy settings on the social networks that they use. If individuals are not clear about how to restrict access to their content, they should regard all content as publicly available and act accordingly.

In using social networking sites, staff are recommended to only post content that they would wish to be in the public domain. Even if content is subsequently removed from a site it may remain available and accessible. Staff should consider not only how content could reflect on them, but also on their professionalism and the reputation of the School as their employer.

Even with privacy settings in place it is still possible that the personal details of staff may be accessed more broadly than the other networkers identified by them. Any reference to such information by pupils and/or their families, which a staff member deems to be inappropriate or is concerned about, should be reported to their line manager in the first instance.

If a member of staff becomes aware that a pupil (or group of pupils) has made inappropriate/insulting/threatening comments about them, or other staff members, on a social networking site; then they must report this to the head teacher so that the appropriate process can be followed.

Preventing Radicalisation

All staff across the school have undertaken 'The Prevent Duty' training. This is to ensure staff awareness of our responsibilities under the Counter-Terrorism and Security Act 2015. It places a duty on specific bodies, such as schools, to 'have due regard to prevent people from being drawn into terrorism.' The intention of training is to increase awareness and understanding about extremism and radicalisation and what to do should concerns arise regarding a child or family. If concerns arise, the matter should be treated as a safeguarding issue and report to the head teacher.

The internet and social media platforms present children and young people with access to a wide range of material, some of which is inappropriate, offensive or harmful. Extremists exploit the internet to radicalise and recruit vulnerable people.

Filtering and content control systems provided by Southampton City Council IT Services block inappropriate content, including extremist material. Social media platforms such as Facebook, Twitter, ect, are also blocked. Where staff, children or visitors find unblocked extremist content, it must be reported to the head teacher.

Staff sign the Acceptable Use of ICT Policy which refers to preventing related radicalisation and extremist content. Parents/Carers sign the Rules for Responsible Internet Use on behalf of the child. Rules are written in child speak and displayed around the school. The Computing Curriculum supports children to make safe choices online and what to do should they come across content that scares or upsets them.

Policy Breaches:

Staff found to be in breach of this policy may be subject to disciplinary action, in accordance with the School's Disciplinary Policy & Procedure and the Code of Conduct and Disciplinary Rules, with potential sanctions up to and including dismissal.

Information shared through social networking sites, even on private spaces, is subject to copyright, data protection, General Data Protection Regulations 2018, freedom of information, equality, safeguarding and other legislation.

Where staff work in roles that are governed by professional bodies/professional codes of conduct; the professional rules relating to social networking applied to them may be more stringent that those within this Policy.

Managing filtering

- Filtering and content control is provided by Southampton City Council IT Services for computers connected to the City network. This uses nationally approved database of keywords and URLs which it filters.
- The school will work with the Local Authority and DfE to ensure systems that protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Computing subject leader and or the Headteacher.
- Staff will ensure that regular 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.
- Staff should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages or files is forbidden.
- Visitors to the school should not use mobile phones/tablets/cameras on the premises and will be challenged by staff if seen to be doing so.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and General Data Protection Regulations 2018.
- All photographs on cameras SD cards or any other recordable device should be downloaded to the relevant folder on the S:/drive/Photographs and then deleted from the card/device at least weekly. All cameras and tablets are recorded as checked and wiped every half term.
- All staff who have a school laptop should only use it for school purposes and no member of their family or friends should have access to this computer.
- Staff who have permission to use remote access should only do so on their allocated school computer.
- Passwords should be memorised and not written down. All data should be stored to the relevant network drive. Computer screens should be locked when leaving them unattended.
- Memory keys and external drives are not permitted to be used.

Policy Decisions

Authorising internet access

- All staff, administration staff, ancillary staff, site managers, students, parents and visitors must read and sign the 'Staff Code of Conduct for Computing' before using any school computing resources.
- All staff and pupils that sign the user agreement will be given access to the internet at school.
- At Key Stage 1 and during the Early Years Foundation Stage, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor Southampton City Council can accept liability for any material accessed, or any consequences of Internet access.
- The Headteacher will ensure that the E-Safety policy is implemented and compliance with the policy is monitored.
- The school will audit Computing use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.
- The use of the computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Handling e-safey complaints
- Complaints of Internet misuse will be dealt with by the Headteacher.
- Any complaint about staff misuse must be referred to the Headteacher.
- The schools complaint procedure will be followed.
- Complaints of a child protection nature must be dealt with in accordance with the school child protection procedures and reported to the Designated Safeguarding Lead.

Communications Policy

Introducing the e-safety policy to pupils
- Pupils will be taught the 'Lock It Block It Show It Tell it' slogan.
- E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly (see appendix). Instruction in responsible and safe use will precede Internet access.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

Staff and the E-Safety Policy
- All staff will be given the School E-Safety Policy and its importance explained.
- Staff will always supervise pupils when using a search engine and help them to select appropriate materials.
- Staff receive annual E-Safety training.
- Staff should complete the e-safety incident report form if they become aware of any e-safety issues in order for the incident to be monitored and dealt with. If the issue is of a child protection nature, it must be dealt with in accordance with the school child protection procedures and reported to the Designated Safeguarding Lead or a Child Protection Lead Officer.

Enlisting parents' and carers' support
- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school web site.
- An e-safety information session will be offered to parents in connection with e-safety day.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.
- If pupils misuse the internet, parents/carers will be informed.

The E-Safety Policy was revised by: Hollie Strudley

Reviewed: March 2019

Next Review: March 2021

Appendix: Acceptable Use of the Internet Policy for schools
Southampton City Council Children's Services and Learning ICT Strategy Team E-Safety Guidance.

Children's Services and Learning ICT Strategy Team

Acceptable use of the Internet Policy

Internet

- Pupils should be supervised at all times when using the Internet. Independent pupil use of telecommunications and electronic information resources is not advised.
- Access to school systems must be with a unique user name and password, which must not be made available to any other staff member or public.
- All Internet activity should be appropriate to staff's professional activity or the student's education.
- Users may use their Internet facilities for non-business research or browsing during meal time breaks, or outside work hours, provided that all other Internet usage policies are adhered to.
- Internet activity that threatens the integrity or security of the school's ICT systems, or activity that attacks, corrupts, or threatens the security of other organisations' systems, is prohibited.
- Copyrights, software licensing rules, laws of the land, property rights, privacy and the rights of others must be respected and adhered to at all times.
- The Intranet/internet must not be used to access, display, store, transmit, distribute, edit or record inappropriate sites such as those containing extremist, terrorist, pornographic, violent, racist, discriminatory, criminal skills related, illegal drugs related or offensive material. Users will recognise materials that are inappropriate and, if deliberately accessing them, should have their access removed.
- The Internet must not be used to download entertainment software or games, or play games against other Internet users.
- Uploading materials or rules to City Council systems must only be performed on machines that have virus protection to the latest corporate standards and with appropriate authorisation from the relevant departments.
- Downloading the files to school systems using file transfer protocol, email and http must be carried out with an appropriate level of care the thought.
- The Internet must not be used to engage in any activity for personal gain or personal business transactions.
- The Internet must not be used to conduct or host any on-going non-education related activities, including discussion groups, chat lines, newsgroups or any other form of on-line club.
- The Internet must not be used for personal or commercial advertisements, solicitations or promotions.
- The use of a school computer system without permission or for a purpose not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.
- To ensure compliance with the acceptable use policy for Web browsing and email. The school reserves the right to monitor and record pupils' activity in these areas. Users

should therefore have no expectation of privacy in respect of their web browsing and email activities when using the school's computer facilities.

- Problems arising from the installation of files, utilities and software updates obtained by such methods are the school's responsibility unless directed to do so by representatives of the City Council or their agents. Virus infection and subsequent removal caused by such methods on machines without protection and the last corporate standards will be the school's responsibility.

Email

- Access to email should only be via the authorised user name and password, which must not be made available to any other staff member or pupil.
- Normally, access to another staff user's email account will not be granted to anyone. However, there are occasions when such access may be legitimately needs, e.g. To aid investigation of suspected irregularities; upon summary dismissal of an employee; during suspension or prolonged absence of an employee; where the retrieval of information is necessary to allow continuation of work in hand by the user whose ID/password combination is to be circumvented.
- Attachments from unknown sources should not be opened, but deleted immediately. All attachments should be scanned for viruses.
- Schools are responsible for all email sent and for contacts made that may result in email being received.
- Pupils must not send/publish their personal details in an email to an unknown recipient.
- Posting anonymous messages and creating or forwarding chain letters is forbidden.
- As email can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Messages that contain abusive or objectionable language, that libel others, or that infringe the privacy rights of others are forbidden.
- Changes must not be made to other people's messages that are then sent on to others without making it clear where the changes have been made.
- Users must not pretend that they are someone else when sending email, or use someone else's account to send a message.
- Users must not publish, electronically or otherwise, any school email address as a point of contact for non-education related activities.
- Personal or otherwise sensitive data must not be transferred via email unless the security of the date whilst in transit can be assured.

Social Networks, Chat Rooms, Instant and Text Messaging

- Pupils should only be given access to secure, age-appropriate chat rooms and social networks, e.g. Grid Club, which are moderated by a teacher, or recognisable, identifiable and approved adult.
- The use of such websites should only be permitted within an educational or professional context.
- Teachers should familiarise themselves with any chat room being used, to ensure that it offers a genuine educational experience.
- Pupils should be supervised at all times when using such websites.
- Pupils should be taught to understand the importance of personal safety on the Internet, i.e. taught never to give out personal contact information or to arrange to meet someone they have met online.

- Access to internet related services such an instant messaging, chat services and social networks is commonplace outside of the school environment. Many young people own, or have access to a mobile phone which increasingly are providing online access. For this reason, schools will need to ensure that pupils are taught safe and responsible behaviours whenever using ICT.

School Websites

- All Southampton City Council school websites will be accessed via a home page provided by the City Council, using the domain name assigned by Nominee i.e. www.schoolname.southampton.sch.uk.
- The production and publication of any unofficial websites is strictly forbidden and if undertaken will be actively pursued by the City Council for removal on behalf of the school.
- A hyperlink will link the official home page to the school website, whether it is hosted with the City Council or externally.
- Only the designated staff member(s) and companies contracted by the school may upload material to the school website and all material for the website must be monitored and approved by the person(s) responsible. The user name and password must not be given to any other members of staff or pupils. If other people know this information, the school should immediately contact CSL ICT Strategy telephone 02380 832111 or email csl.ict@southampton.gov.uk to have the password changed.
- Images of pupils and staff should be classed as personal data under the terms of the Data Protection Act 1998. Therefore using such images for school publicity purposes, i.e. school website will require the consent of either the individual concerned or in the case of pupils, their legal guardians.
- Recognisable photography, full names, addresses, telephone numbers and email addresses of pupils must not be published on the school website. Home addresses and telephone numbers of school staff, parents and governors should not be published on the school website, where possible the school details should be given as the main point of contact.
- Southampton City Council reserves the right to remove any material from school websites if it is considered to be unsuitable or if it poses a threat to the safety of a school or pupil.

Staff Code of Conduct for Computing

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Member of staff should consult the school's e-safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school Co system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones. PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school purposes.
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will not access, display, store, transmit, distribute, edit or record inappropriate sites such as those containing extremist, terrorist, pornographic, violent, racist, discriminatory, criminal skills related, illegal drugs related or offensive material.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not use any social networking sites (eg Facebook, Twitter, MySpace) to bring the name of the school or any of its staff into disrepute. I will not share any pupil information or comment about them when using social network sites.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Headteacher.
- I will not communicate with pupils electronically (ie e-mail, IM, social networking) and any electronic communication with parents will be done using the schools e-mail system.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imaginary or sound.

I have read, understood and accept the Staff Code of Conduct for Computing.

Name..... Signature.....

Date..... Position in school.....

Fairisle Infant & Nursery School

Fairisle Road
Lordshill
Southampton
SO16 8BY
Telephone: (023) 8073 1199
Facsimile: (023) 8073 9099

Headteacher: Mrs. S. Ottens, B.Sc.(Hons.), P.G.C.E., N.P.Q.H.

Dear Parent/Carer

Use of the Internet and e-mail in Schools

As part of the school's Computing programme, we offer pupils supervised access to the Internet and e-mail. Before the school allows students to use these facilities, they must obtain parental permission. Both pupils and parents must sign and return an Internet Use Permission Form as evidence of their acceptance of the school's Rules for Responsible ICT Use. Copies of both are enclosed with this letter.

Various projects have proven the educational benefits of Internet and e-mail access, which enable pupils to explore a wide range of information sources, and communicate and collaborate with other learners throughout the world. Although there are concerns about children having access to inappropriate material via the Internet, the school takes a range of measures to minimise these risks. A filtering system is in operation, which restricts access to inappropriate materials, and this is supplemented by an Internet safety programme for all pupils, which teaches the safe and appropriate behaviours to adopt when using the Internet, e-mail and other technologies.

Whilst every measure is taken to ensure the suitability of material, Southampton City Council cannot be held responsible for the nature or content of materials accessed through the Internet. Southampton City Council will not be liable under any circumstances for any damages arising from your child's use of the Internet facilities.

Although Internet use is supervised and filtered within our schools, families should be aware that some pupils may find ways to access material that is inaccurate, defamatory, illegal or potentially offensive to some people. As with any other area, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources.
During school, teachers will guide students towards appropriate material. At home, families bear the same responsibility for guidance as they exercise with other information sources such as television, telephones, films and radio.
In order to allow your child access to the internet at school, please read the attached Rules for Responsible Computing Use, complete and sign the enclosed permission form and return it by the end of term. The school has a number of internet addresses from national bodies that explain issues further and also cover Internet use a home. If you would like copies of these, please contact the school.

If you require further guidance or advice on the use of the Internet, or would like to discuss any other related issues, please do not hesitate to telephone to arrange an appointment.

Yours sincerely

S. Ottens

Mrs Susanne Ottens
Headteacher

Please complete and return this form to the school office

Parent/Carer

I have read and discussed the school rules for responsible Computing use with my child, and as the parent or legal guardian of the pupil signing above, I grant permission for my son or daughter to use the Internet, e-mail and other Computing facilities at school. I understand that the school will take reasonable precautions to ensure that pupils can not access inappropriate materials, including the teaching of Internet safety skills to pupils, but accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet. I accept responsibility for setting and conveying standards for my son or daughter to follow when selecting, sharing and exploring information and media, and acknowledge that they will be deemed to be accountable for their own actions.

Parent/Carers signature: _____ *Date:* _____

Pupil's name: _____

Class: _____

Rules for Responsible Internet Use

These rules will help us to be fair to others and keep everyone safe.

- I will ask permission before using the Internet.
- I will not look at or delete other people's files.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- I will not give my home address or phone number, or any personal information, or arrange to meet someone.
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I don't know.
- If I see anything I am unhappy with or I receive a message I do not like, I will tell a teacher immediately.
- I understand that the school may check my computer files and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.