NORFOLK CHILDREN'S SERVICES
Mousehold Infant & Nursery School

Title of Policy:
E-Safety

Subject Leader/Contact Person:

Ian Tolson

This policy has been developed, reviewed & adopted as follows:

	Date of Draft	Date Agreed	Date of Review	Date of Review	Date of Review
Staff	Sep 2016	Sept 2016	Sept 2017	Sept 2018	
Governors		Sept 2016	Sept 2017		

School Aims:	Respect, Help, Learn, Enjoy, Achieve.
School Self Evaluation:	• How high are standards? • Pupils' attitudes, values & personal development. • How well are pupils taught? • How good are curricular & learning opportunities? • How well does the school care for its pupils? • How well is the school led & managed? • How well does the school work in partnership with parents? • How effective is the school?

Signed ………………………… (Headteacher)

Signed …………………………(Governor)

Mousehold Infant and Nursery School E-safety Policy

To underpin the values and ethos of our school and our intent to ensure our children/young people are appropriately safeguarded this policy is included under the safeguarding umbrella. It also relates to the ICT policy.

What is E-Safety?

E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones, games consoles and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The safe and effective use of the Internet is an essential life-skill, required by all. However, unmediated Internet access brings with it the possibility of placing users in embarrassing, inappropriate and even dangerous situations.

Much of the material on the Internet is published for an adult audience and some is unsuitable for children. In addition, there is information on weapons, crime and racism, access to which would be more restricted elsewhere. Children and young people must also learn that publishing personal information could compromise their security and that of others.

The school's e-Safety coordinator is Ian Tolson. Our e-Safety Policy has been written by the school, building on the Norfolk e-Safety Policy and government guidance.

It has been agreed by the leadership team and approved by governors.

The e-safety policy and its implementation will be reviewed annually.

Alongside this policy, the school adheres to Norfolk County Council 'Internet and e-mail in schools: model guidance for schools staff, and all staff are required to sign the staff code of conduct (acceptable use) for ICT schools.

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.

How can we safely use the Internet to enhance learning?

The school Internet access is designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use through rules and responsibilities and safe computer use guidance.

Pupils will be taught how to evaluate Internet content

In a perfect world, inappropriate material would not be visible to pupils using the Internet, but despite filtering this is not easy to achieve and cannot be totally guaranteed. Through guidance on safe computer use, children are told what to do if they see anything on the internet that they are uncomfortable with.

All online materials will be evaluated before use.

The school will endeavour ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

Managing Internet Access

Information system security

School ICT systems capacity and security will be reviewed in accordance with Becta Framework for IT support.

Virus and Spyware protection will be installed and updated regularly.

Security strategies will be discussed with Systems Solutions and guidance will be sought from the LA.

Once a secure server has been established, log in details will not be shared.

Email

It is unlikely that children will be sending e-mails individually and unsupervised. However, the following guidance should be followed.

Pupils may only use approved e-mail accounts.

Pupils must immediately tell a teacher if they receive an unexpected e-mail.

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

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.

Staff should not contact pupils or parents using personal e mail addresses

Published content and the school web site

The contact details on the Web site are the school address, e-mail and telephone number. Staff or pupils personal information will not be published.

The Deputy Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Photographing pupils and publishing pupil's images and work

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

Pupils' full names will not be used anywhere on the Web site or particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site

Staff should refer to model guidance for school staff regarding the use of personal cameras and other ICT devices such as mobile phones to photograph children (3.6 and 3.10)

Work can only be published with the permission of the pupil and parents.

Guidance is available at http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/taking_photos_v3.0_final.pdf.

Social networking and personal publishing

The LA / School will block/filter access to inappropriate social networking sites.

Staff must not access social networking sites for personal use via school information systems or using school equipment.

Newsgroups will be blocked unless a specific use is approved.

If relevant, pupils will be advised never to give out personal details of any kind which may identify them or their location.

The learning platform is an appropriate place to communicate electronically with students when relevant skills have been taught.

Staff should not communicate with parents or children using public social networking sites such as Facebook, MySpace, Twitter, etc.

It is inappropriate for pupils of primary age to use Social Network sites.

Further guidance on the use of social networking sites can be found in Section 4 of the Internet and e-mail use in schools; model guidance for staff.

Managing filtering

The school will work in partnership with the LA and Systems Solutions to ensure systems to protect pupils are reviewed and improved.

If pupils discover an unsuitable site they should inform the teacher immediately. Any unsuitable sites must be reported to **Ian Tolson (**E-Safety coordinator), who will inform the Network Manger and ICT Solutions.

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, and the view of the Advisory Service and ICT Solutions shall be sought.

Children are not permitted to bring ICT devices into school, such as mobile phones, without the permission of the Headteacher.

The school allows staff to bring in personal mobile phones and devices for their own use. Staff are not allowed to use their mobile phones when on duty or in lesson time. Staff are not allowed to take photos of children at school on their personal devices. Class cameras and ipads should only be used for this. Staff should not be contacting pupils or parents/carers using their personal devices.

The sending of inappropriate messages by SMS or any other communication system or technology between any members of the school community is not allowed (For definition of Inappropriate refer to "ICT Code of Conduct")

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 the school E-safety policy and Internet and e mail use in schools: model guidance for staff. They must read and sign the 'Staff Code of Conduct' before using any school ICT resource.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor NCC can accept liability for the material accessed, or any consequences of Internet access.

The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is effective.

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 Headteacher. Further guidance about the consequences of unacceptable use of internet, email and equipment can be found in section 6 of the model guidance for staff on internet and e mail use in schools for staff.

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

Safeguarding

Safeguarding is everyone's responsibility at Mousehold and all members of staff adhere to our Child Protection and Safeguarding Policy. We feel it is important to remember why children behave the way they do and this does affect their learning. We expect all staff to read and follow the guidelines set out in the ' Keeping Children Safe in Education 2018' document. This can be found in the Staff Handbook in the staffroom. It can also be found online.

Extract from our Child protection and Safeguarding Policy – PREVENT STRATEGY

We recognise that safeguarding against radicalisation and extremism is no different to safeguarding against any other vulnerability in today's society. At Mousehold Infant and Nursery School, we will ensure that:

- Through training, staff, volunteers and governors have an understanding of what radicalisation and extremism is, why we need to be vigilant in school and how to respond when concerns arise.
- There are systems in place for keeping pupils safe from extremist material when accessing the internet in our school by using effective filtering and usage policies.
- The DSL has received Prevent training and will act as the point of contact within our school for any concerns relating to radicalisation and extremism.
- The DSL will make referrals in accordance with Norfolk Channel procedures and will represent our school at Channel meetings as required.

Communications Policy

Introducing the e-safety policy to pupils

Safe use of computer rules will be posted in all classrooms.
Users will be informed that network and Internet use will be monitored.

Staff and the e-Safety policy

All staff will be shown the School e-Safety Policy together with the internet and e-mail guidance for school staff, and its importance explained. A copy will be put into safeguarding folders.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

Parents'/Carers' attention will be drawn to e-Safety in newsletters and on the website. All new parents will be asked to sign an e safety agreement when they register their child with the school.

Parents/carers will be directed to CEOP (Child exploitation and online protection centre) in order to access one-stop shop website for internet safety and advice.