Kinsale Infant School
Online Safety Policy

To underpin the values and ethos of our school and our intent to ensure our children are appropriately safeguarded, this policy is included under the safeguarding umbrella. It also relates to our ICT policy and the new Relationship Education curriculum.

What is online safety?

Online safety encompasses not only internet technologies, but any form of electronic device, platform or app. 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 online safety coordinator is **Lisa Hazard**. Our Online Safety Policy has been written by the school, building on the Norfolk e-Safety Policy and current government guidance from 2019. It has been agreed by the leadership team and approved by governors. The Online Safety Policy and its implementation will be reviewed annually.

Alongside this policy, the school adheres to Norfolk County Council 'Internet and e-mails in schools: model guidance for schools staff' and all staff are required to sign the staff code of conduct (acceptable use) for ICT in 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 children with quality internet access as part of the learning experience. It is essential that children are provided with the knowledge and understand of appropriate behaviours so that they have positive experiences online.

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. The teaching of online safety is in an age-appropriate way that is relevant to the children's experiences. Online safety is embedded throughout the whole school through the use of assemblies, and referring to the online safety posters displayed during teaching and learning time..

Pupils will be taught how to evaluate internet content

All online materials will be evaluated before use. The school will endeavour to ensure that the use of internet derived materials by staff and by pupils complies with the copyright law.

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 safety online, children are told what to do if they see anything on the

internet that they are uncomfortable with. Teaching online safety provides children with the skills they need to help them evaluate what they see online, such as considering whether a website is fake.

Any pupil can be vulnerable online, and this can fluctuate depending on factors such as the child's age or developmental stage. However, it is important that the school is aware that some children who are more susceptible to online harm, such as those with special educational needs or looked after children. It is important that the school tailors their teaching to ensure these children receive the support and knowledge that they need.

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. Our ICT technician ensures this takes place. Security strategies will be discussed with ICT Solutions and guidance will be sought from the LA. Once a secure server has been established, log in details will not be shared.

Published content and the school website

The contact details on the website are the school address, e-mail and telephone contact number. Staff or pupils personal information will not be published. The Head teacher, supported by the Deputy Head teacher 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 website or particularly in association with photographs. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or in the press.

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 be published with the permission of the pupil and parents.

Guidance is available at:
http://www.ico.gov.uk/uplaod/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.
Staff should not communicate with our school parents or children using any public social networking sites such as Facebook, MySpace etc.
It is inappropriate for pupils of primary age to use Social Networking sites. This is tackled with parents if appropriate.
Further guidance on the use of social networking sites can be found in Section 4 of the internet and email use in schools; model guidance for staff.

Managing Filtering

The school will work in partnership with the LA and ICT Shared Services to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator or the ICT technician (In Touch ICT).

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 Shared Services shall be sought.
Children are not permitted to bring ICT devices into school, such as mobile phones, without the permission of the Head teacher.

The school allows staff to bring in personal mobile phones and devices for their own use. Staff should not be contacting parents/carers using their personal devices. Mobile phones are not to be used near children (this applies to staff and visitors, and notices are displayed to explain this).
The sending of inappropriate messages by SMS or any other communication system or technology between any members of the school community is not allowed.

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 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 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 Online 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 Head teacher. 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 email use in schools for staff.
Complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures.

Communications Policy

Introducing the online safety policy to pupils

Safe use of computer rules are posted in the ICT suite and all classrooms.

Staff and the online safety policy

All staff will be shown the school online safety policy together with the internet and email guidance for school staff, and its importance explained.
Staff should be made 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 online safety in the school brochure and on the website.

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 if appropriate.

September 2019
Review Date : September 2020
Signed by Chair of Governors: P Steward
Date: 30.9.19