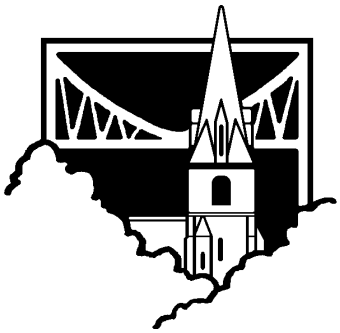

North Ferriby C E Primary School

E-Safety Policy
(Staff, Parents and Pupils)

Date of New Policy:	**Summer 2018**
Review Date:	**Summer 2020**
Policy Type:	**School**
Co-ordinator:	**Mr Orr**
Link Governor:	**Derek Shepherd**

North Ferriby CE Primary School Mission Statement:

A Christian School with children at its heart.

Christian Values Statement:

At North Ferriby CE Primary School, we keep Christian values at the heart of our school community where we live, love and learn together.

Ethos Statement for North Ferriby CE VC Primary:

Recognising its historic foundation, the school will preserve its religious character in accordance with the principles of the Church of England and in partnership with the Church at parish and diocesan level.

The school aims to serve its community by providing an education of the highest quality within the context of Christian belief and practice.

It encourages an understanding of the meaning and significance of faith and promotes Christian values through the experience it offers to all its pupils.

YORK DIOCESAN BOARD OF EDUCATION

Introduction

The internet has become increasingly accessible for children who will experiment online. Learners need opportunities to create, collaborate in and explore the digital world, using multiple devices from multiple locations. However, all users need to be aware of the range of risks associated with the use of these internet technologies alongside the development of safe and responsible online behaviours.

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 at North Ferriby Primary School is to raise educational standards, to promote pupil's achievement and to support the professional work of staff.

The benefit to pupils of internet use

A number of studies and government projects have identified that there are benefits to be gained through the appropriate use of the Internet. These benefits include:

- access to world-wide educational resources including museums and art galleries
- professional development for staff through access to national developments, educational materials and effective curriculum practice

Enhancing learning and life experiences

Pupils learn digital literacy skills and to refine their publishing and communications with others via the Internet. Pupils are taught:

- Respect for copyright and intellectual property rights, as well as the correct use of published material
- To use the internet enhance and extend education
- What does and doesn't constitute acceptable use of the internet.
- to use the internet effectively for research, including the skills of choosing search terms, retrieval and evaluation
- To acknowledge the sources of any information used, and to respect copyright when using material found on the internet in their own work

Evaluating content

The internet offers easily accessible age inappropriate material. Pupils are taught to evaluate content critically. This includes the intent and accuracy of information received via email, text or through social media, as the contextual clues may be missing or difficult to read. Pupils are taught to be critical of the materials they read and shown how to validate information before accepting its accuracy. The evaluation of on-line materials is a part of teaching/learning in every subject.

Maintenance of information systems and security.

Data is defined as: numerical or other information represented in a form suitable for processing by computer.

The Head teacher is in charge of data security but all staff with access to personal data are liable by law to protect that data. Should data be lost from an unencrypted USB drive or seen

on a laptop used by other people, the consequences could be serious for the member of staff, for the school.

Local Area Network (LAN) security procedures include:

- Access to all ICT systems shall be via unique login and password
- Where possible, all information storage is restricted to only necessary users
- All teachers will have access to pupil folders, however requests for access beyond that normally allocated, are authorised by the head teacher
- Where 'restricted' information is stored, access is only granted to individuals approved by the head teacher
- All access controls are reviewed annually, to ensure that any users that leave have their access removed
- Workstations are secured against user mistakes. This is to prevent that access and security being compromised
- Servers are located securely and physical access is restricted
- The server operating system is secured and kept up to date
- Virus protection for the whole network is current and updated when necessary
- Access by wireless devices is pro-actively managed and password protected
- Portable media (eg USB drives) is not used without a virus check
- The person in charge of network management will review system capacity regularl
- Files held on the school network are pro-actively managed.

Filtering

Levels of Internet access and supervision vary according to the pupil's age and experience. We use Smoothwall filtering systems to ensure that systems to protect pupils are reviewed and improved. Requests for filtering changes will be directed to our technical support contractors.

Management of emerging technologies

Many emerging technologies offer the potential to enhance new teaching and learning, including mobile communications, collaboration and the development of multimedia tools. A risk assessment is undertaken on each new technology to ensure access is secure and no compromises occur. Access is denied until a risk assessment has been completed and safety established.

Protection of Personal Data

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals.

The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

Securing Passwords

Only members of staff have access to ICT systems. They are responsible for taking the appropriate steps to select and secure their passwords.

Staff must:

- keep their passwords secure from others.
- use a different password in school to that used for personal purposes.
- choose a password that is difficult to guess, or difficult for others to obtain by watching them login.
- adding numbers or special characters (e.g. !@£$%^).

All workstations are set up so that log in is needed after the computer is left any length of time (for example during break and lunchtimes)

Management of email

- Pupils only use approved email accounts in school
- Pupils immediately tell an adult if they receive offensive email
- Pupils are taught not reveal personal details of themselves or others
- Staff use all use school e-mails for all professional communication.

Management of Published Content

- The contact details on the website are the school name address, email and telephone number. Employee or pupil's personal information is not published.
- The head teacher has overall editorial responsibility and ensures that content is accurate and appropriate
- The website complies with our guidelines for publications including respect for intellectual property rights, copyright and the privacy rights of individuals.

Publication of pupil images and work.

Pupils are taught the reasons for caution in publishing personal information and images online.

- Pupil's full names are not be used anywhere on the website
- Written permission from parents or carers is obtained before images of Pupils are electronically published
- Pupil's work can only be published with their permission or the permission of the parent/carer

Management of Social Networking

- Access to social media and social networking sites is blocked in school
- Pupils are taught 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
- Pupils are taught not to place personal photos on any social network space
- Pupils are taught to consider how public the information is and consider using private areas. Advice is given regarding background detail in a photograph which could identify the child or young person or his/her location
- Pupils are taught to consider the affect, publishing information about others will have
- A secure internal 'social network' space exists for pupils to use within the limits of the VLE
- Personal publishing, through blogs and web design is through the secure limits of the VLE. Children are taught not to publish personal information and the site is moderated by staff
- Pupils are taught about security and shown how to set passwords, deny access to unknown individuals and instructed how to block unwanted communications

- Pupils are encouraged to invite known friends only and deny access to others by making profiles private
- Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Authorisation of Internet Access

- Use of the internet in school is fully supervised
- Parental permission is obtained for Internet access
- School maintain a log of all parent consent forms
- All classroom based staff have read and signed the e-safety, safeguarding and acceptable use policies
- Pupils are granted Internet access only after agreeing to and signing the Acceptable Use Policy annually
- Parents/carers are informed that pupils are provided with supervised and Internet access, and countersign the children's Acceptable Use Policy

Assessment of Risk

Disclaimer:

- North Ferriby Primary 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 computer. Neither the school nor ERYC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit digital technological use annually 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.

Handling of Parental Complaints:

- Complaints of Internet misuse is dealt with under the school's Complaints Procedure
- ANY COMPLAINT ABOUT STAFF MISUSE MUST BE REFERRED TO THE DESIGNATED SAFEGARDING LEAD (DSL) IN THE FIRST INSTANCE
- All e–safety complaints and incidents are recorded by the DSL, including any actions taken
- Pupils and parents/carers are informed of the complaints procedure
- School works in partnership with parents/carers, and pupils to resolve issues
- Any issues (including sanctions) are dealt with according to our disciplinary and child protection procedures

Management of Cyber Bullying

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" (DCSF 2007).

- Cyberbullying (along with all forms of bullying) is not tolerated in our school. (See anti-bullying policy)
- There are clear procedures in place to support anyone affected by cyberbullying
- All reported incidents of cyberbullying are recorded
- There are clear procedures in place to investigate incidents or allegations of cyberbullying:

The head teacher keeps a record of the bullying as evidence.

Steps are taken to identify the bully, where appropriate, such as examining system

logs, identifying and interviewing possible witnesses, and contacting the service provider and if necessary, the police,

Sanctions for those involved in cyberbullying may include:

- The bully is asked to remove any material deemed to be inappropriate or offensive
- A service provider may be contacted to remove content
- Internet access/ VLE access may be suspended for the user for a period of time
- Parents/carers are informed.

The Police will be contacted if a criminal offence is suspected.

Management of Learning Platforms and VLEs

- Staff monitor the usage of the VLE by pupils, parents and staff regularly in all areas, in particular message and communication tools and publishing facilities
- Pupils, parents and staff are advised on acceptable conduct and use when using the learning platform
- Only pupils, parents/carers, staff and governors have access to the VLE
- All users mindful of copyright issues and only upload appropriate content onto the VLE
- When pupils, parents and staff leave the school their account or rights to specific school areas is disabled or transferred to their new establishment
- Any concerns with content is recorded and dealt with in the following ways:

a) The user is asked to remove any material deemed to be inappropriate or offensive.
b) The material is removed by the site administrator if the user does not comply.
c) Access to the VLE for the user may be suspended.
d) The user will need to discuss the issues with a member of e-safety team before reinstatement.
e) A pupil's parent/carer is informed.

Response to an Incident of Concern

All pupils, parents and staff have a responsibility to report e-safety or e-security incidents so that they may be dealt with effectively and in a timely manner in order to minimise any impact. School has an incident reporting procedure and records reported incidents in an Incident Log.

The Incident Log is formally reviewed, and any outstanding actions delegated, by the DSL within school at a minimum frequency of once per term. If appropriate, risk assessments will be updated following new incidents.

The Log and accompanying action plans are reviewed annually by the Governing Body through the 'Safeguarding Report to Governors'.

It is acknowledged that there are people other than the school staff who can help. Online child abuse can be reported directly, as well as requests to seek out more advice and support. Reports can be made directly to CEOP through their Click CEOP reporting button, which is present on an increasing number of websites and social networks.
http://www.ceop.police.uk/

Introduction of the Policy to Pupils

Pupils will be introduced to the eSafety policy through the Acceptable use policy in specific lessons. The Acceptable Use Policy will be countersigned by parents as part of the Home/School agreement.

Involvement of Staff

Consideration is given when staff are provided with devices which may be accessed outside of the school network. Staff are made aware of the safe and appropriate use of such equipment and rules about use of this by third parties. Staff are made aware of their responsibility to maintain confidentiality of school's information. All staff including administrators, governors, and parents are included in awareness raising and training. Induction of new staff/volunteers includes training in school's e–safety Policy. The e–safety Policy has been formally provided to and discussed with all members of teaching staff and governors. Staff are aware that Internet traffic is monitored and can be traced to the individual user.

Parental Support

E-safety is taken seriously both at home and in school. Parents are offered training courses in awareness of e-safety and internet use.

Parents'/carers' attention is drawn to the e-safety Policy in newsletters, the prospectus and on the website as well as through the Child Protection Policy and Procedures. A partnership approach with parents/carers is encouraged including parent evenings with demonstrations and suggestions for safe home Internet use.

Parents/carers are requested to sign an e–safety/internet agreement as part of the Home School Agreement. Information and guidance for parents/carers on e–safety is made available to parents/carers via the school website.