# SHANKLEA PRIMARY SCHOOL

## E-Safety Policy

| Policy Control Details | | | |
|---|---|---|---|
| Date policy approved: | September 2020 | | |
| Prepared by: | Senior Leadership Team | Signature | Date |
| Approved for issue by: | Gareth Pearson | Signature | Date |
| Review period: | 1 year | | |
| Review required by: | September 2021 | | |
| Responsibility for review: | Performance Improvement Committee | | |

## E-Safety Policy

E-Safety encompasses not only Internet technologies but also electronic communications via 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.

- E-safety concerns safeguarding children and young people in the digital world.
- E-safety emphasizes learning to understand and use new technologies in a positive way.
- E-safety is less about restriction and more about education about the risks.
- E-safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

The school's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security.

The following policies should be read in conjunction with this document:

Staff Acceptable Use Policy, (including wi-fi acceptable use)

Pupil Acceptable Use Policy

Parents and Carers Acceptable Use Policy

Parents and Carers Leased iPad Acceptable Use Policy (for parents leasing iPads through school)

Staff Code of Conduct

Staff Social Networking Acceptable Use Policy

## End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the NCC including the effective management of web filtering.
- National Education Network standards and specifications.

# School e-safety policy

### 2.1 Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.

I. The school has appointed an e-Safety coordinator, Mrs L.aura Greenwood
II. Our e-Safety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors.
III. The e-Safety Policy and its implementation will be reviewed annually.
IV. The e-Safety Policy was reviewed by: Mrs H Brown and Mrs L Greenwood.
V. It was initially approved by the Governors on: June 2016

## 2.2 Teaching and Learning

### 2.2.1 Why Internet use is important

I. 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.
II. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
III. 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.

### 2.2.3 Internet use will enhance learning

I. The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
II. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
III. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

### 2.2.4 Pupils will be taught how to evaluate Internet content

I. Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
II. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
III. Pupils will be taught how to stay safe when working online.

## 2.3 Managing Internet Access

### 2.3.1 Information system security

I. School ICT systems capacity and security will be reviewed regularly.

II. Virus protection will be installed and updated regularly.

III. Security strategies will be discussed with the Local Authority.

### 2.3.2 E-mail

I. Pupils may only use approved e-mail accounts on the school system.

II. Pupils must immediately tell a teacher if they receive offensive e-mail.

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

IV. 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.

V. The forwarding of chain letters is not permitted.

VI. Staff should only use school email accounts to communicate with pupils as approved by the Senior Leadership Team.

VII. Staff should not use personal email accounts during school hours or for professional purposes

### 2.3.3 Published content and the school web site

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

II. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

### 2.3.4 Publishing pupil's images and work

I. Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. An exception is the school newsletter which may include some photographs to celebrate pupil achievement where parental permission has been given.

II. Pupils' full names will not be promoted anywhere on the Web site, particularly in association with photographs.

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

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

### 2.3.5 Social networking and personal publishing

I. School will block/filter access to social networking sites.

II. Newsgroups will be blocked unless a specific use is approved.

III. Pupils will be advised never to give out personal details of any kind which may identify them or their location.

IV. All staff should be made aware of the potential risks of using social networking sites or personal

publishing either professional or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Staff should refer to the Staff Acceptable Use Policy and the Staff Code of Conduct.

V. Examples include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chat rooms, instant messenger and many others.

#### 2.3.6 Managing filtering

I. The school will work in partnership with the Local Authority, Department for Children Schools and Families and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

II. If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator.

III. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

#### 2.3.7 Managing videoconferencing

I. IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.

II. Staff will set up and monitor any videoconference calls.

III. Videoconferencing will be appropriately supervised for the pupils' age.

#### 2.3.8 Managing emerging technologies

I. Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

II. If pupils require the use of a mobile phone before or after school it can be stored in the office during the day.

III. Staff will be issued with a school phone where contact with pupils is required.

IV. No staff or visitor mobiles are allowed around the building. The office and staffroom areas are designated for staff mobile use.

#### 2.3.9 Protecting personal data

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

## 2.4 Policy Decisions

#### 2.4.1 Authorising Internet access

I. All staff must read and sign the 'Staff Acceptable Use Policy' and 'Staff Code of Conduct' before using any school ICT resource.

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

III. At EYFS, Key Stage 1, Out of School Club and Lunchtime Clubs access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

IV. At Key Stage 2 pupils will have some access to the ICT suite on approved sites only.

V. Pupils and parents will be asked to sign and return the Parents Acceptable Use Policy and Pupils Acceptable Use Policy.

**2.4.2 Assessing risks**

**I.** 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.

**II.** 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 appropriate.

**2.4.3 Handling e-safety complaints**

I. Complaints of Internet misuse will be dealt with by a senior member of staff.

II. Any complaint about staff misuse must be referred to the headteacher.

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

IV. Pupils and parents will be informed of the complaints procedure.

V. Links will be established with Community Police Officer to seek advice when necessary.

**2.4.4 Community use of the Internet**

The school will liaise within the Cramlington Partnership to establish a common approach to e-safety.

**2.4.5 Cyber bullying**

I. Cyber bullying (along with all forms of bullying) will not be tolerated in school.

II. All incidents of cyber bullying reported to the school will be recorded.

**2.4.6 The Learning Platform (LP)**

I. SLT and staff will monitor the usage of the LP by pupils and staff regularly in all areas, in particular message and communication tools and publishing facilities.

II. Pupils/staff will be advised on acceptable conduct and use when using the learning platform.

III. Only members of the current pupil, parent/carers and staff community will have access to the LP.

IV. When staff, pupils etc leave the school their account or rights to specific school areas will be disabled.

## 2.5 Communications Policy

### 2.5.1 Introducing the e-safety policy to pupils

I. e-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.

II. Pupils will be informed that network and Internet use will be monitored.

III. The Parents Acceptable Use Policy and the Pupils Acceptable Use Policy will be sent home for parents and children to discuss, sign and return to school.

### 2.5.2 Staff and the e-Safety policy

I. All staff will be given the School e-Safety Policy and its importance explained.

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

III. Staff will be given the Staff Acceptable Use Policy and Staff Code of Conduct to read and sign.

### 2.5.3 Enlisting parents' support

I. Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

## 2.6 Acceptable Use Policies

2.6.1 There are separate Acceptable Use Policies for Pupils, Staff, Parents and Carers and an additional policy for Parents and Carers in the Leased iPad Scheme. There is also a Staff Social Networking Acceptable Use Policy which provides guidance for those staff administering school social media accounts.

2.6.2 The Acceptable Use Policy for Pupils aims to ensure that pupils use IT systems and computers safely, access only appropriate materials, and protect themselves and Shanklea Primary School from possible risks. It is written in language appropriate to the age of children so that they may understand it fully.

2.6.3 Acceptable Use Policies aim to balance the desirability of fully exploiting the vast educational potential of Information Technology and Internet resources for learning and communication, with safeguards against any risks and unacceptable activity. Non compliance will be immediately reported to Mrs L Greenwood (E Safety Co-ordinator or Mrs Brown (Head teacher) and may result in disciplinary action.

## 2.7 Security

When required, pupils will be allocated usernames and passwords to access school computers and systems. Pupils must not use a password belonging to another person or attempt to access files where they have not been authorised. Pupils must not gain or attempt to gain unauthorised access to any computer. Such hacking or attempted hacking is a criminal offence under the Computer Misuse Act 1990. The following is not permitted in school IT equipment without permission form the Head teacher or E Safety Co-ordinator:-

- Changes to installed software or hardware
- Downloading and/installing software on school equipment

## 2.8 Internet Access and Use

All pupil Internet access must be via the school's wired or wireless network and on a device that has been configured by the IT services department.

Pupils must not, by using the school's service, possess or transmit illegal material. Pupils should be aware that some activities/material which may be legal in the UK may be illegal in other parts of the world and vice versa.

Downloading certain files can introduce viruses and other security threats onto the network; therefore some file types might be blocked.

Internet access throughout school is filtered and monitored and supervised by the school and Northumberland county council. If you come across a site which contains offensive material you must report this immediately to your teacher so that the site can be blocked.

If pupils directly refer to Shanklea Primary School on any internet website all comments should be within school rules that require pupils to be responsible, thoughtful and considerate.

## 2.9 Removable Storage Media

Use of encrypted removable storage media (e.g. USB pens) is allowed only when no additional software is needed.

## 2.10 Digital Media Storage

Personal picture files and images must not be stored on the network. Personal audio and video files must not be stored on the network either. School work related media files may be stored on the network.

## 2.11 Cyber Bullying

This is defined as bullying by use of e-mail, mobile phone and text messages, instant messaging, personal websites and/or chat rooms. Any suspected cyber bullying (whether during school time or otherwise) will be reported immediately to the Head Teacher, Mrs Brown or Mrs Greenwood (E Safety Coordinator).

## 2.12 Mobile Phones

The use of mobile phones during school time is limited to the office and staffroom areas. Phones are not allowed around school.

If pupils require the use of a mobile phone before or after school it can be stored in the office during the day.

Coaches and other visitors need to leave their phones at the office.

## 2.13 Email Accounts

When required pupils will be allocated an email account. These accounts are for restricted use only within school. User names and passwords are not to be shared.

## 2.14 Monitoring ICT Usage

Forensic software is used to tightly monitor all ICT and technological usage on the recommendations of the ICT Department of Northumberland County Council.

**I have read and understood and agree to comply with the E-Safety Policy.**

Signed: ……..... Print Name: ……. Date: ……

Accepted by: ……..…….. Print Name: ……..…….