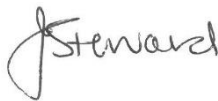





## ONLINE SAFETY POLICY

Formally adopted by the Governing Body of Sheringham Community Primary & Nursery School	
On	23 <sup>rd</sup> November 2023
Chair of Governors	
Head Teacher	
Last updated	23 <sup>rd</sup> November 2023
Review	23 <sup>rd</sup> November 2024

*Be all that you can be...*



## Contents

1. Writing and reviewing the Online Safety Policy .....	3
2. Teaching and learning .....	3
2.1. Why Internet and digital communications are important .....	3
2.2. Pupils will be taught how to evaluate Internet content .....	3
3. Managing Internet Access.....	3
3.1. Information system security.....	3
3.2. E-mail.....	4
3.3. Published content: the School Website, Facebook and Twitter account ....	5
3.4. Publishing photographs, images and work .....	5
3.5. Social networking and personal publishing.....	5
3.6. Managing filtering.....	5
3.7. Managing emerging technologies .....	6
3.8. Other devices .....	6
3.9. Protecting personal data.....	6
4. Policy Decisions.....	6
4.1. Authorising Internet access.....	6
4.2. Assessing risks .....	7
4.3. Classification of Online Risks - the 4Cs.....	7
4.4. Handling Online Safety complaints .....	7
4.5. Community use of the Internet .....	7
5. Communications Policy.....	7
5.1. Introducing the Online Safety Policy to pupils .....	7
5.2. Staff and the Online Safety Policy .....	8
5.3. Enlisting parents' support .....	8

## 1. Writing and reviewing the Online Safety Policy

The Online Safety Policy relates to other policies including those for the curriculum, bullying and safeguarding.

- The school's Designated Safeguarding Lead (DSL) has overall responsibility for Online Safety. They are supported by the Computing Coordinator who, alongside the ICT technician, monitors Online Safety across the school including all school online security systems.
- Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors
- The Online Safety Policy and its implementation will be reviewed annually
- Online Safety training is given to all staff on a regular annual basis.

## 2. Teaching and learning

### 2.1. Why Internet and digital communications are 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.
- Internet use is a part of the curriculum and a necessary tool for staff and pupils.
- The school Internet access is provided by TalkStraight and includes filtering appropriate to the age of pupils. This system is called Netsweeper.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet
- Pupils will be shown how to publish and present information appropriately to a wider audience.

### 2.2. Pupils will be taught how to evaluate Internet content

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content e.g. reporting to a trusted adult in the first instance, as well as Childline and using the CEOP Report Abuse icon.

## 3. Managing Internet Access

### 3.1. Information system security

- School ICT systems will be monitored regularly to identify unauthorised access and potential malicious network activity.
- To monitor the schools internet activity, reports generated from the TalkStraight Netsweeper internet filtering system will be reviewed daily by the Deputy Head and Head Teacher.
- Virus protection will be updated regularly. This is also purchased annually to ensure the best possible virus product.
- Security strategies will be discussed with the leadership team and DSL to ensure they meet current guidelines
- All staff will use the appropriate username and passwords to ensure system security. It is their responsibility to ensure that they maintain security and control of these. Copies of these are kept in a locked safe at school and in a password protected section on the school server.
- All staff are responsible for any data that they carry between school and home. This data should be password protected and not stored on a home system.

All school data with the exception of the MIS information is stored on the school server. The server is located in a secured air conditioned room at Woodfields School. A network attached backup device is located in the core communications cabinet at Sheringham Primary School and in accordance with current data protection recommendations all backup data is safely secured with password protected data encryption.

In the event of fire at Woodfields School, data can be recovered from the network attached backup located at Sheringham Primary School. And, in the event of fire at Sheringham Primary School, data can be accessed from the school server located at Woodfields School.

- All confidential data which the Senior Leadership Team wish to kept separate is stored on a password protected area of the school server. Only those with the appropriate access can use this feature.
- All information systems are managed using an administrator account, which can only be used by the School System Administrator (Mr P Guymer).

### **3.2. E-mail**

- Pupils and staff may only use approved NSIX e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff to pupil email communication must only take place via a school email address or from within the school learning platform (such as Google Classroom) and will be monitored by the designated Computing Coordinator and the DSL.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

- The school will consider how e-mail from pupils to external bodies is presented and controlled.

### **3.3. Published content: the School Website, Facebook and Twitter account**

- The contact details on the Website, Facebook and Twitter accounts should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.

### **3.4. Publishing photographs, images and work**

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by their name unless with full permission of the parents. The school will look to seek to use group photographs rather than full-face photos of individual children.
- Pupils' full names will be avoided on the Website, Facebook and Twitter as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs or images of pupils are published.
- Written permission from adults will be obtained before their names, photographs or images of themselves are published.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

### **3.5. Social networking and personal publishing on the school learning platform**

- The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords.
- All users will be advised never to give out personal details of any kind which may identify them, anybody else or their location.
- Pupils, parents and staff will be advised on the safe use of social network spaces
- Staff will be advised of their roles and responsibilities under the pay and conditions of service. This includes appropriate use of social media and how it could be viewed.
- Pupils will be advised to use nicknames and avatars when using social networking sites.

### **3.6. Managing filtering**

- The school will work in partnership with Norfolk Children's Services to ensure systems to protect pupils are reviewed and improved. This system is called Netsweeper
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the nominated members of staff (DSL and Computing Coordinator.)

- The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. This is carried out on a weekly and half termly basis.

### **3.7. 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.

### **3.8. Other devices**

- Only school owned cameras/devices can be used for taking photographs/videos in lessons and educational activities and visits.
- Staff will secure their personal devices and not use them during designated teaching time.
- Staff will use school phones for trips and school devices for photographs. Personal devices must only be used in an absolute emergency.
- The sending of abusive, offensive or inappropriate material is forbidden. Such events will be investigated by the designated persons under the appropriate code of conduct
- Staff should not share personal telephone numbers or contact details with pupils and parents as part of their role. (A school phone will be provided for staff where contact with pupils is required).

### **3.9. Protecting personal data**

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and our Data Protection Policy.

## **4. Policy Decisions**

### **4.1. Authorising Internet access**

- All staff must read and sign the 'Staff Code of Conduct' and 'Acceptable Use Policy' 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.
- Parents will be asked to sign and return a consent form.
- Pupils must agree to comply with the Responsible Internet Use statement before being granted Internet access.

#### 4.2. **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 Norfolk Children's Services can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate and effective.

#### 4.3. **Classification of Online Risks - the 4Cs**

The 4Cs classification recognises that online risks arise when a child:

- engages with and/or is exposed to potentially harmful CONTENT;
- experiences and/or is targeted by potentially harmful CONTACT;
- witnesses, participates in and/or is a victim of potentially harmful CONDUCT;
- is party to and/or exploited by a potentially harmful CONTRACT/COMMERCE.

#### 4.4. **Handling Online Safety complaints**

- Complaints of Internet misuse by children will be dealt with by the DSL and Headteacher who will be assisted by the Computing Coordinator.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be referred to the DSL and dealt with in accordance with school's child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

#### 4.5. **Community use of the Internet**

- All use of the school Internet connection by community and other organisations shall be in accordance with the school Online Safety policy. Staff will also follow the relevant staff code of conduct sections.

### 5. **Communications Policy**

#### 5.1. **Introducing the Online Safety policy to pupils**

- Appropriate elements of the Online Safety policy will be shared with pupils
- Online Safety rules will be posted in all networked rooms, where there is pupil use of a computer.

- Pupils will be informed that network and Internet use will be monitored
- The issues around Online Safety are specifically planned for as part of the curriculum content in each year group

### 5.2. **Staff and the Online Safety policy**

- All staff will be given the School Online Safety Policy and its importance explained
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff who manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

### 5.3. **Enlisting parents' support**

- Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will from time to time be provided with additional information on Online Safety, which includes yearly learning café meetings.
- Parents receive Online Safety updates on the school Facebook and Twitter pages via [Nationalonlinesafety.com](http://Nationalonlinesafety.com)
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school and again in at the start of Key Stage 2.