



# **Sheerness West Federation**

## **e-SAFETY POLICY**

March 18

Review: March 19

*"Dreams Come True With A Positive View"*

<b>Policy Review Process</b>	
Frequency of Review	<b>Annually</b>
Reviewed	<b>March 18</b>
Reviewed By	FLT
Next Review Date	March 19

<b>Policy Status</b>	<i>Non-Statutory</i>
----------------------	----------------------

<b>Policy Approval</b>			
<b>Policy to be approved by:</b>		<i>Governing Body</i>	
<b>Title</b>	<b>Name</b>	<b>Signed</b>	<b>Dated</b>
Chair of Governing Body	Mr D Goodwin		
Executive Head	Mr S Davies		
Head of Schools	Miss H Brewer		
Date Policy Ratified by Governing Body / FLT			10/07/2018

### Document Storage

This document is stored electronically as detailed below:

- On KLZ Sharepoint where it is accessible to all SWF Staff
- On the shared network drive, accessible to FLT members only
- On the school website(s) where applicable

A hardcopy of this document is kept in the FLT Offices at Rose Street and West Minster Primary Schools.

## Contents

Our Vision .....	4
Overview.....	4
Teaching and Learning .....	4
Why Internet use is important .....	4
Internet use will enhance learning .....	5
Pupils will be taught how to evaluate Internet content .....	5
Managing Internet Access .....	5
Information system security .....	5
E-mail.....	5
Published content and the school Websites .....	6
Publishing children’s images and work .....	6
Social networking and personal publishing .....	6
Managing filtering .....	6
Managing video conferencing .....	7
Managing emerging technologies .....	7
Protecting personal data .....	7
CCTV Use within school .....	8
Storage and movement of information .....	8
Policy Decisions.....	8
Authorising Internet access.....	8
Assessing risks .....	8
Handling e-safety complaints.....	8
Communications Policy.....	9
Introducing the e-safety policy to children.....	9
Staff and the e-safety policy.....	9
Enlisting parents’ support.....	9

## Our Vision

At the Sheerness West Federation we recognise that learning is a life long journey. Our creative and nurturing environment supports all children through their journey, aspiring each individual in becoming confident, successful independent learners. We aim for all our children to actively engage in a learning experience which inspires, motivates and challenges them. We are an inclusive Federation where the diversity that exists amongst us is celebrated and aids our deeper understanding of the world we live in. We have high expectations of all our children and work in close partnership with all members of the Federation community to build successful, resilient, responsible citizens of the future.

## Overview

E-Safety encompasses Internet technologies and electronic communications such as mobile 'phones and tablets as well as collaboration tools and personal publishing. It highlights the need to educate children about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The previous Online Safety Policy has been revised and renamed as the Federation e-Safety Policy to reflect the need to raise awareness of the safety and privacy issues associated with electronic communications as a whole.

**Our e-Safety Policy builds on the Kent e-Safety Policy and EU General Data Protection Regulation (GDPR) due to be enforced from May 2018. This policy will be continually reviewed to ensure compliance with GDPR.**

The Federation will follow the **UK Council for Child Internet Safety (UKCCIS) –“The Education for a Connected World framework” (2018)** which describes the Digital knowledge and skills that children and young people should have the opportunity to develop at different ages and stages of their lives. It highlights what a child should know in terms of current online technology, its influence on behaviour and development, and what skills they need to be able to navigate it.

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

e-Safety is a Federation-wide responsibility. Co-ordination for and implementation of this policy lies with Designated Safeguarding Leads, e-safety Lead Teachers, ICT Lead Teachers, IT Manager, the Full Leadership Team and Governors.

## 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 their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and children.

*“Dreams Come True With A Positive View”*

Children use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter.

### **Internet use will enhance learning**

The Federation Internet access is and will be designed expressly for pupil use and includes filtering appropriate to the age of the children.

Children will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of children.

Staff should guide children in on-line activities that will support the learning outcomes planned for the children's age and maturity.

Children will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

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

The Federation will ensure that the use of Internet derived materials by staff and children complies with copyright law.

Children should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Children will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

## **Managing Internet Access**

### **Information system security**

Federation computing systems capacity and security will be reviewed regularly.

Virus protection will be updated regularly.

Security strategies will be discussed with KCC/EIS.

### **E-mail**

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

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

Children 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 parents / carers or any external organisation both by children as part of a lesson, or by staff, should be written carefully and, where necessary, authorised before sending, in the same way as a letter written on school headed paper. The forwarding of chain letters is not permitted.

### **Published content and the school Websites**

The contact details on the websites should be the school address, e-mail and telephone number. Staff or children's personal information will not be published.

The Full Leadership Team will take overall editorial responsibility and ensure that content is accurate and appropriate and that statutory content is up to date.

### **Publishing children's images and work**

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

Children's full names will not be used anywhere on the websites or Blog, particularly in association with photographs.

Signed consent from parents or carers will be obtained before photographs of children are published on the school website.

Children's work can only be published with the permission of the child and parents.

### **Social networking and personal publishing**

The Federation will block/filter access to social networking sites.

Newsgroups will be blocked unless a specific use is approved.

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

Children and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

The school Facebook pages are closely monitored. Any material which the Federation finds offensive will be removed, investigated and action taken as appropriate.

Federation staff will not use personal social network spaces, ie "Facebook" to engage with parents / carers, staff or volunteers regarding school issues. Staff training will include advice around confidentiality and who they are "friends with" on social networking spaces and how this may impact on school.

### **Managing filtering**

The Federation will work with LEA, DfES and the Internet Service Provider to ensure systems to protect children are reviewed and improved.

*"Dreams Come True With A Positive View"*

If staff or children discover an unsuitable site, it must be reported to the Designated Safeguarding Leads / e-Safety Leads.

The Full Leadership Team and IT Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

### **Managing video conferencing**

IP video conferencing, e.g. SKYPE, Facetime, etc. should use KPSN – Schools Broadband with LightSpeed Filtering to ensure quality of service and security rather than the Internet.

Children should ask permission from the supervising teacher before making or answering a videoconference call.

Video conferencing will be appropriately supervised for the children's age.

### **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.

Personal mobile 'phones will not be used by staff in or during lessons or in areas of the school where children are present. Staff use of personal mobile 'phones will be restricted to staff rooms / PPA room and offices.

Only children in Year 6 who walk to and from school will be allowed to bring mobile 'phones into school and these will be left in the school office on arrival at school and collected at the end of the day.

Staff will not use any "app" on a personal mobile 'phone to communicate with children or parents.

Staff will not access work emails via a personal mobile 'phone without the approval of the Federation IT Manager.

Children are not allowed to take mobile 'phones to off-site activities organised by the Federation. The sending of abusive or inappropriate text or other messages or emails is forbidden.

Staff will only use school landline 'phones where contact with children or parents is required. Staff on school trips will use a school mobile 'phone or make contact with parents via the school.

### **Protecting personal data**

Personal data will be recorded, processed, transferred and made available according to **GDPR (2018)** regulations.

## **CCTV Use within school**

CCTV is used within each school for the safety and security of staff and children, as well as safeguarding the premises. Visitors and members of the Federation will be made aware of the CCTV used within the school and screened appropriately (See separate CCTV policy).

## **Storage and movement of information**

Information stored within the school will be stored securely on Federation servers in line with KCC guidelines. Security of data stored in all non-Federation platforms are subject to an agreed contract with, and is overseen by, the service provider.

Movement of data will take place only via encrypted pen drives. No data shall be emailed externally, unencrypted or via unsecure providers. All laptops, tablets and mobile devices will be password protected. Personal staff smart 'phones or other devices used to access Federation emails must be password protected.

## **Policy Decisions**

### **Authorising Internet access**

All staff must read and sign the E-Safety agreement before using any school computing resource.

The Federation will keep a record of all staff (including student teachers) and children who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

Parents will be asked to sign and return a consent form.

### **Assessing risks**

The Federation will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a Federation computer. Neither the Federation nor KCC can accept liability for the material accessed, or any consequences of Internet access.

The Federation will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly.

### **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 Executive Head Teacher.

Complaints of a safeguarding (child protection) nature must be dealt with in accordance with Federation safeguarding policy and procedures.

Parents and children will need to work in partnership with staff to resolve issues.

## **Communications Policy**

### **Introducing the e-safety policy to children**

Child friendly e-Safety rules are posted in all networked rooms with Internet access and around each school. These rules are discussed with the children at the start of each year.

Children will be continually reminded that network and Internet use will be monitored. Ongoing e-Safety awareness reminders are given during IT and other relevant lessons.

### **Staff and the e-safety policy**

All staff will be given the Federation e-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 training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

### **Enlisting parents' support**

Parents' attention will be drawn to the Federation e-Safety Policy in newsletters, the school prospectus and on the individual school Websites.

All e-safety issues will be handled sensitively, and parents will be advised accordingly.