Foxfield School

 E Safety Policy

This policy is due for review on June 2022



**Contents**

School eSafety Policy 1

Why is Internet use important? 1

How does Internet use benefit education? 1

How Can Internet Use Enhance Learning? 1

Authorised Internet Access 2

World Wide Web 2

Email 2

Social Networking 2

Filtering 3

Video Conferencing 3

Managing Emerging Technologies 3

Published Content and the School Web Site 3

Publishing Students’ Images and Work 3

Information System Security 3

Protecting Personal Data 4

Assessing Risks 4

Handling eSafety Complaints 4

Communication of Policy 4

Students 4

Staff 4

Parents 4

Appendix 5

Appendix A 6

Appendix B 7

Appendix D 8

Appendix E 9

Appendix F 10

Appendix G 11

 Appendix H ……………………………………………………………………...12

Updated 22/07/2019

# e-Safety Policy

eSafety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school’s eSafety policy will operate in conjunction with other policies including those for Behaviour and Discipline, Bullying, Curriculum, Data Protection and Security.

Foxfield School has an ICT co-ordinator Mr Ian Harwood. Part of his role is the responsibility for safety.

## *Why is Internet use important?*

The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school’s management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for all our students. Our school has a duty to provide students with quality Internet access and support them in this use.

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

## *How does Internet use benefit education?*

Benefits of using the Internet in education include:

* Access to learning wherever and whenever convenient
* Access to world-wide educational resources
* Educational and cultural exchanges between students world-wide
* Access to experts in many fields for students and staff
* Professional development for staff through access to national developments, educational materials and effective curriculum practice;
* Collaboration across support services and professional associations;
* Improved access to technical support including remote management of

networks and automatic system updates;

Exchange of curriculum and administration data with the Local Authority and DCSF

**How can internet use enhance learning?**

* The school Internet access will be designed expressly for student use and includes filtering appropriate to the age of students
* Students 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.
* Staff should guide and supervise students in on-line activities that will support learning outcomes planned for the students’ age and ability
* Students will be educated in the effective use of the Internet.

## *Authorised Internet Access*

* The school will maintain a current record of all staff and students who are granted Internet access
* All staff must read and sign the ‘Acceptable ICT Use Agreement’ before using any school ICT resource
* Parents will be informed that students will be provided with supervised Internet access

## *World Wide Web*

* If staff or students discover unsuitable sites, the URL (address), time, content must be reported to Deputy Headteacher, the technician, the RM provider and recorded in the eSafety log.
* Foxfield School will ensure that the use of Internet derived materials by students and staff complies with copyright law
* Individual students and web sites can be locked out using the filter system if specific students persistently access inappropriate internet material

## *Email*

* Students may only use approved e-mail accounts on the school system
* Students must immediately tell a teacher if they receive offensive e-mail
* Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
* Staff must supervise and where possible vet all e-mail communications sent by the students using the school system.
* The forwarding of chain letters is not permitted

##

## *Social Networking*

* The School will block/filter access to social networking sites and newsgroups unless a specific use is approved
* Students will be advised if using sites at home and in school, never to give out personal details of any kind which may identify them or their location
* Students should be advised not to place personal photos on any social network space
* Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others

## *Filtering*

The school will work in partnership with the Local Authority to ensure filtering systems are as effective as possible.

## *Video Conferencing*

* Pupils should ask permission from the supervising teacher before making or answering a videoconference call and a member of staff present.
* Videoconferencing will be appropriately supervised for the pupils’ age and ability.

## *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
* Mobile phones/ handheld communications devices/ gaming consoles will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

## *Published Content and the School Web Site*

* The contact details on the Web site will be the school address, e-mail and telephone number. Staff or pupils personal information will not be published
* The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

## *Publishing Students’ Images and Work*

* Photographs that include students will be selected carefully and will be appropriate for the context
* Students’ full names will not be used anywhere on the Web site, particularly in association with photographs
* Written permission from parents or carers will be obtained before photographs of students are published on the school web site
* Photographs of LAC will not be published on the internet.

## *Information System Security*

* School ICT systems capacity and security will be reviewed regularly
* Virus protection will be installed and updated regularly
* Security strategies will be discussed with the Local Authority

## *Protecting Personal Data*

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

## *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 Wirral Metropolitan Borough Council can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT use to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate.

## *Handling eSafety 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 Headteacher.
* Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. Pupils and parents will be informed of the complaints procedure

## *Communication of Policy*

### Students

* Students will be informed that Internet use will be monitored

### Staff

* All staff will be given the School eSafety 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 that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues

### Parents

* Parents’ attention will be drawn to the School eSafety Policy in newsletters, the school brochure and on the school Web site.

# Appendix

#

1. Questions we will use to evaluate the effectiveness of our policy in meeting its aims are
2. Our annual review tool
3. Responding to incidents
4. ESafety Rules
5. Pupil Esafety Acronym
6. Staff Code of Conduct
7. Esafety Audit
8. Esafety Incident Log

# Appendix A

# Questions we will use to evaluate the effectiveness of our policy in meeting its aims are:

## Policies and practice

* Does the school have a set of robust policies and practices?
* Do you have an acceptable use policy (AUP)? Is everyone aware of it?
* Does your anti-bullying policy include references to cyberbullying?
* Are there effective sanctions for breaching the policy in place?
* Have you appointed an e-safety co-ordinator?

## Infrastructure

* Is the school network safe and secure?
* Do you use an accredited internet service provider?
* Do you use a filtering/monitoring product?

## Education and training

* Do children receive e-safety education – where, how?
* Are staff – including support staff – trained?
* Do you have a single point of contact in the school?
* Do the leadership team and school governors have adequate awareness of the issue of e-safety?

# Appendix B

# Our annual review tool

# Are you an eSafe school?

|  |  |
| --- | --- |
| Do all your staff... ⬜ Understand e-safety issues and risks? ⬜ Receive regular training and updates? ⬜ Know how to escalate an issue of concern? ⬜ Know how to keep data safe and secure? ⬜ Know how to protect themselves online? ⬜ Know how to conduct themselves professionally online? ⬜ Know about the updated e-safety guidance for QTS standard Q21: Health and well-being?  | Does your school... ⬜ Have a nominated e-safety co-ordinator? audit its e-safety measures? ⬜ Have a robust AUP? ⬜ Use a Becta accredited supplier for internet services? ⬜ Include e-safety measures in Section 4b of your SEF? ⬜ Keep an incident log and monitor your measures? ⬜ Handle cyberbullying issues well? ⬜ Raise awareness of the issues, e.g. through holding an assembly?  |
| Do your learners... ⬜ Understand what safe and responsible online behaviour means? ⬜ Receive e-safety education at appropriate places across the curriculum? ⬜ Get the opportunity to improve their digital literacy skills? ⬜ Know the SMART rules? ⬜ Know how to report any concerns they may have?  | Do your parents and governors... ⬜ Understand e-safety issues and risks? ⬜ Understand their roles and responsibilities? ⬜ Receive regular training and updates? ⬜ Understand how to protect their children in the home?  |

## Appendix C

Flowchart for responding to eSafety incidents in school

#

eSafety Incident

Inappropriate Activity

Unsuitable materials

#

Report to Headteacher

Contact

 Headteacher

If staff: review incident and decide on appropriate course of action, applying sanctions as necessary

If student: review incident and decide on appropriate course of action, applying sanctions as necessary

Debrief

Review policies and technical tools

Implement changes

Monitor

Adapted from Becta – eSafety 2005

## Appendix D

**eSafety Rules**

These eSafety Rules help to protect students and the school by describing acceptable and unacceptable computer use.

* The school owns the computer network and can set rules for its use.
* It is a criminal offence to use a computer or network for a purpose not permitted by the school.
* Irresponsible use may result in the loss of network or Internet access.
* Network access must be made via the user’s authorised account and password, which must not be given to any other person.
* All network and Internet use must be appropriate to education.
* Copyright and intellectual property rights must be respected.
* Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
* Anonymous messages and chain letters are not permitted.
* Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
* The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
* Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school will exercise its right to monitor the use of the school’s computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school’s computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Think Before You Click

Use these rules to stay safe when using the Internet

|  |  |
| --- | --- |
| Sj0233806 | I will only use the Internet and email with an adult |
| Aj0285374 | I will only click on icons and links when I know they are safe |
| Fj0316779 | I will only send friendly and polite messages |
| Ej0292020 | If I see something I don’t like on the screen, I will always tell an adult |

|  |
| --- |
| My Name |
| My Signature |

##

## Appendix F

Staff Information Systems Code of Conduct

**To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school’s eSafety policy for further information and clarification.**

* The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
* I will ensure that my information systems use will always be compatible with my professional rôle.
* I understand that school information systems may not be used for private purposes, without specific permission from the Headteacher.
* I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
* I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
* I will not install any software or hardware without permission.
* I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
* I will respect copyright and intellectual property rights.
* I will report any incidents of concern regarding children’s safety to the school eSafety Coordinator or the Designated Child Protection Coordinator.
* I will ensure that any electronic communications with students are compatible with my professional rôle.
* I will promote eSafety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school’s information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school’s information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.**I have read, understood and agree with the Information Systems Code of Conduct.**

Signed: ………………………… Printed: ……………………… Date: ………

Accepted for school: ……………………………. Capitals: ………………

## Appendix G

ESafety Audit

This quick self-audit will help the senior management team (SMT) assess whether the eSafety basics are in place.

|  |  |
| --- | --- |
| Has the school an eSafety Policy that complies with CYPD guidance?  | **Y/N** |
| Date of latest update: |
| The Policy was agreed by governors on: |
| The Policy is available for staff at:  |
| And for parents at: |
| The designated Child Protection Teacher/Officer is:  |
| The eSafety Coordinator is:  |
| Has eSafety training been provided for both students and staff? | **Y/N** |
| Is the Think U Know training being considered?  | **Y/N** |
| Do all staff sign an ICT Code of Conduct on appointment?  | **Y/N** |
| Do parents sign and return an agreement that their child will comply with the School eSafety Rules?  | **Y/N** |
| Have school eSafety Rules been set for students?  | **Y/N** |
| Are these Rules displayed in all rooms with computers? | **Y/N** |
| Is Internet access provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access?  | **Y/N** |
| Has the school filtering policy been approved by SMT?  | **Y/N** |
| Is personal data collected, stored and used according to the principles of the Data Protection Act?  | **Y/N** |
| Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SMT?  | **Y/N** |

## Appendix H

eSafety Incident Log

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Staff | Incident | Action |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Policy Agreement and Review**

**Policy Ratified at Full Governors:**

Signed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
(Headteacher) (Chair of Governors)
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |
| --- | --- | --- |
| **Review Date** | **Reviewed by** | **Amendments made** |
|  |  |  |
|  |  |  |
|  |  |  |

**LITERATURE BASE**

Taken from ‘Safeguarding Children Online’ Becta February 2009

<http://publications.becta.org.uk/download.cfm?resID=39409>