



St John Fisher RC Primary School

Acceptable Internet Use and E-Safety Policy

MISSION STATEMENT

**Love Jesus, love learning,
Inspiring each other to be the best that we can be.**

Introduction

Access to the Internet is a necessary tool for staff and students. The purpose of Internet access is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems.

Usually, the resources used by pupils in school are carefully chosen by the teacher and determined by curriculum policies. Whilst pupils will be directed to sites which provide reviewed and evaluated sources, at times, they will be able to move beyond these, to sites unfamiliar to the teacher.

The problems and issues that have been highlighted by the media concern all schools. Whilst some of the media interest is hype, there is genuine cause for concern that children might access unsuitable material either accidentally or deliberately.

The purpose of this policy is to:

- Establish the ground rules we have in school for using the Internet
- Describe how these fit into the wider context of our discipline and PHSE policies
- Demonstrate the methods used to protect the children from sites containing pornography, racist or politically extreme views and violence

The school believes that the benefits to pupils from access to the resources of the Internet far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians.

At St John Fisher, we feel that the best recipe for success lies in a combination of site-filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

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 pupils with quality Internet access as part of their learning experience.

The benefits of using the internet include:

- access to a wide variety of educational resources including libraries, art galleries and museums
- rapid and cost effective world-wide communication
- gaining an understanding of people and cultures around the globe
- staff professional development through access to new curriculum materials, experts' knowledge and practice
- exchange of curriculum and administration data with LEA/DFE
- social and leisure use.

The school intends to teach pupils about the vast information resources available on the Internet, using it as a planned part of lessons. E-Safety will be taught to all pupils from Reception and will be readdressed throughout the year and also as part of lessons. Sessions will be taught using age appropriate resources and will include the following areas: Email, SMS Messaging, Social Networking and Cyber Bullying.

Older pupils will have the opportunity to exchange information via email. They will be taught how to use the address book, how to attach files to an email and how to follow conventions of politeness. Pupils will only learn how to use an e-mail application once they have been taught the Rules of Responsible Internet Use and agreed their Acceptable User Policy.

As pupils gain experience, they will be taught how to use searching techniques to locate specific information. Comparisons will be made between researching from different sources of information, (Books, WWW). We hope that pupils will learn to decide when it is appropriate to use the Internet, as opposed to other sources of information, in terms of: the time taken; the amount of information found; the usefulness and reliability of information located.

Using information from the Internet

We believe that, in order to use information from the Internet effectively, it is important for pupils to develop an understanding of the nature of the Internet and the information available on it.

In particular, they should know that, unlike the school library for example, most of the information on the Internet is intended for an adult audience, much of the information on the Internet is not properly audited or edited and most of it is protected.

Pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV.

Teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true.

When copying materials from the Web, pupils will be taught to observe copyright; pupils will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed.

Pupil's Access to the Internet

St John Fisher School will only allow children to use the Internet when there is a responsible adult present to supervise. However, it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen. Children are not allowed to use the computers during wet playtimes / dinnertimes.

Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils, the expectation we have of pupils.

Teachers will have access to pupils' emails and other Internet related files and will be able to check these on a regular basis if necessary, to ensure expectations of behaviour are being met.

Microsoft Teams

Microsoft Teams is used as Learning Platform as a means to set online learning for pupils. The IT Technician and Teachers use Microsoft Teams to set tasks for children to complete task in school or at home.

Staff should ensure that they establish safe and responsible online behaviours, working to local and national guidelines and then schools acceptable use policy when using Microsoft Teams.

Communication with children and adults, by whatever method, should take place within explicit professional boundaries and staff should avoid any personal subject matter. Staff should not request or respond to any personal information from children other than that which may be necessary in their professional role. They should ensure that their communications are open and transparent and avoid any communication which could be interpreted as 'grooming behaviour'.

Staff should not give their personal contact details to children for example, e-mail address, home or mobile telephone numbers, social media information, or details of web based identities. If children locate these by any other means and attempt to contact or correspond with the staff member, they should not respond, report the matter to the Headteacher and the child and their parents should be firmly and politely informed that this is not acceptable.

When communicating with children on Microsoft Teams, adults should:

- Not seek to communicate/make contact or respond to contact with pupils outside of the purpose of their work and should not accept any requests for contact from pupils outside of the workplace
- Not give out their personal details
- Use only equipment and Internet services provided by the school or setting, unless school policies state otherwise
- Only use internet-enabled personal devices in line with school acceptable use policies
- Follow their school Acceptable Use Policy and online safety guidance
- Ensure that their use of technologies could not bring their employer into disrepute.

Seesaw

Seesaw is used as Learning Platform as a means to set online learning for pupils. Teachers use Seesaw to set tasks for children to complete task in school.

Staff should ensure that they establish safe and responsible online behaviours, working to local and national guidelines and then schools acceptable use policy when using Seesaw.

Communication with children and adults, by whatever method, should take place within explicit professional boundaries and staff should avoid any personal subject matter. Staff should not request or respond to any personal information from children other than that which may be necessary in their professional role. They should ensure that their communications are open and transparent and avoid any communication which could be interpreted as 'grooming behaviour'.

Staff should not give their personal contact details to children for example, e-mail address, home or mobile telephone numbers, social media information, or details of web based identities. If children locate these by any other means and attempt to contact or correspond with the staff member, they should not respond, report the matter to the Headteacher and the child and their parents should be firmly and politely informed that this is not acceptable.

When communicating with children on Seesaw, adults should:

- Not seek to communicate/make contact or respond to contact with pupils outside of the purpose of their work and should not accept any requests for contact from pupils outside of the workplace
- Not give out their personal details
- Use only equipment and Internet services provided by the school or setting, unless school policies state otherwise
- Only use internet-enabled personal devices in line with school acceptable use policies
- Follow their school Acceptable Use Policy and online safety guidance
- Ensure that their use of technologies could not bring their employer into disrepute.

Prevent Duty: Tackling Radicalisation and Extremism

The Prevent strategy aims to protect vulnerable people from being drawn into terrorism. While it remains rare for children and young people to become involved in terrorist activity, young people from an early age can be exposed to terrorist & extremist influences or prejudiced views. We recognise that as with other forms of safeguarding strategies, early intervention is always preferable. Our school is committed to working with other local partners, families and communities, and we will play a key role in ensuring young people and their communities are safe from the threat of terrorism.

We also recognise that our School has a duty of care to our pupils and staff which includes safeguarding them from the risk of being drawn into terrorism. Being drawn into terrorism includes not just violent extremism but also non-violent extremism, which can create an atmosphere conducive to terrorism and can popularise views which terrorists exploit. Prevent can work within both violent and non-violent extremism arenas and can include topics such as hate crime, racism, bullying, on line safety and extreme political views.

Our School is committed to:

- Managing access to extremist material- ICT filters.
- Responding to any allegations appropriately in accordance with appropriate school policies and procedures (see Tackling Radicalisation and Extremism Policy)

Publishing pupil's images and work

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

Pupils' 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 pupils are published on the school Web site.

Social networking and personal publishing

The school will block/filter access to some social networking sites.

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

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

Staff are advised that the use of social networks is not permitted in school and should not be accessed using the school network.

Managing filtering

The school will work with the Rochdale Local Authority Schools ICT Unit, Edit, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the Computing Coordinator and Rochdale Local Authority Schools ICT Unit and Edit.

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

Fortinet is the management filter. This is managed by Edit.

Assessing risks

The school 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 school computer. Neither the school nor Rochdale Local Authority can accept liability for the material accessed, or any consequences of Internet access.

If there is an incident in which a pupil is exposed to offensive or upsetting material, the school will wish to respond to the situation quickly and on a number of levels:

- Staff will log the event with the Computing Co-ordinator;
- A letter will be sent home to inform parents;
- Discussion to take place with all parties.

Introducing the E-safety policy to pupils

E-safety rules will be posted in all classrooms and discussed with the pupils at the start of each year.

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

Staff and the E-Safety policy

All staff will be given the School 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.

Enlisting parents' support

Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school website.

Document history

Date	Amendments
September 2015	Amended for new curriculum
October 2015	Added information regarding Prevent Duty
September 2017	Reviewed
September 2019	Reviewed
April 2020	See-Saw section added to policy
September 2020	Microsoft Teams section added to policy
September 2021	Reviewed
September 2022	Reviewed
September 2023	Reviewed
September 2024	Reviewed
September 2025	Reviewed