Fairfield School
Embracing Uniqueness

Online-Safety Policy

Version	Version 2.0
Date reviewed:	November 2021
Review date:	November 2023
Approved by Governors:	23 November 2021

Online-Safety Policy (Including Acceptable Use Policy Guidelines)

The purpose of internet use at Fairfield school is to raise educational opportunities and promote achievements, support the professional work of staff and enhance the school's management of information, communication and administration systems between staff, pupils, parents or carers. Therefore, safeguarding children and young people online can involve a range of potential issues such as cyber bullying, extremist behaviour, grooming, child sexual exploitation etc. This highlights the need to educate pupils, their parents, carers and staff about the benefits and risks of using this environment and provide safeguards and awareness for users to safely control their online experiences.

Introduction

At Fairfield Online -Safety encompasses Internet technologies and also electronic communications such as mobile phones, games consoles and wireless technology. It highlights the need to educate our pupils (where appropriate) about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to control their online experiences. In addition, it ensures that correct measures are in place to deal with breaches of Online-safety.

The safe and effective use of the Internet is an essential life skill; however, internet access brings with it the possibility of placing users in inappropriate and even dangerous situations.

An effective E-safety policy will address these issues and ensure that all staff and pupils are following the Acceptable Use guidelines. In addition, it will ensure appropriate security measures are in place to protect the school network and filter out inappropriate material.

Pupils are not permitted to bring ICT devices into school without permission. The school allows staff to bring in personal mobile phones which may be used in the staffroom, away from the pupils. Staff should not be contacting pupils or parents/carers using their personal devices.

The school's Online-Safety lead is Tanzila Ilyas, who is also the Designated Safeguarding Lead.

Issues regarding E-safety, particularly those relating to child safeguarding, should be reported to Tanzila Ilyas, John Page, Lucy Roche or Rachel Holmes

The E-safety policy and its implementation will be reviewed annually.

Legislation and Guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education. and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

Relationships and sex education

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given staff powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

Roles and Responsibilities

The Governing Body

The governing body has overall responsibility for monitoring this policy and holding the SLT to account for its implementation.
The governing body will co-ordinate with the SLT to discuss and monitor online safety. The governor with reasonability for safeguarding and who oversees online safety is Mandy Farrar.

The DSL

Details of the DSL and deputies are set out in our safeguarding policy 2021 and any complaints of Internet / staff misuse must be referred to the SLT
The DSL takes lead responsibility for online safety in school:

- Supporting the Head teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school, and addressing on line safety training needs
- Working with the Head teacher, ICT Network Manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 1) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Providing regular reports on online safety in school to the headteacher and/or governing board

Teaching and Learning

The Internet is an essential element in 21st century life for education. Fairfield School has a duty to provide our pupils with quality Internet access as part of their learning experiences. Access to the Internet has been shown to increase motivation and engagement of pupils, particularly those with special or additional needs.

How can we safely use the Internet to enhance learning?

The school Internet access is designed expressly for pupil use and will include filtering appropriate to the suitability of the pupils. Access levels will be reviewed to reflect curriculum requirements and suitability of pupils.
Pupils will be taught (where appropriate) what Internet use is acceptable and what is not and will be given a clear set of rules for using the computers and internet in school. Pupils will have clear objectives for Internet use, through planned activities which guide pupils and support the learning outcomes.

Pupils will be taught how to evaluate Internet content

The school will endeavour to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law, including encouraging pupils to acknowledge sources.
Pupils (where appropriate) will be taught to be aware of the material they read and taught how to validate information before accepting its accuracy

Managing Internet Access

How will the information system's security be maintained?

The security of the school information system will be reviewed by the ICT Network Manager, reporting to the SLT. Virus and Spyware protection will be installed and updated regularly. Security strategies will be discussed with ICT Services, where applicable. Any login details will not be shared. Passwords to access the administration of the network will be kept by the ICT Manager. Written details of passwords will be kept locked in the safe. Portable media may not be used by staff to transfer work from home to school in line with school regulations regarding pupil data use. If a member of staff suspects a concern with a school device, they must let the ICT Network Manager know as soon as possible. The ICT Network Manager will review the system capacity regularly.

How will E-mails be Managed?

Pupils must not reveal personal details of themselves or others in e-mail communication, or make arrangements to meet anyone.
Staff should not contact pupils or parents using personal e-mail addresses; they are advised to use their Fairfield School address when dealing with school based issues whenever possible.

What is Cyber-Bullying?

Cyber-bullying is the use of digital technologies with an intent to offend, humiliate, threaten, harass or abuse somebody. It can come in a whole range of different shapes and sizes.
It can leave children and young people feeling scared, upset, isolated and vulnerable, particularly as the bullying can happen anywhere, at anytime
There are a number of different methods of cyber-bullying. The main ones include:

- Electronic communication such as messages, texts, e-mails, photographs, video-messaging, sexting via mobile phones, computers, smart-phones, tablets etc to individuals or groups
- Communication is threatening, upsetting or offensive and may include racist, sexist, or homophobic content
- Making humiliating and abusive phone calls on mobiles or land lines
- Sending inappropriate communication that can be shared with others through social networking and gaming sites
- Communicating with friends of the victim and other people to try to include them in the bullying
- Setting up 'profiles' on social networking sites to make fun of a child or young person
- Creating a false identity to impersonate someone and send inappropriate communications in their name
- Use chat rooms and gaming sites to abuse other players, use threats, lock victims out of games, spread false rumours
- Sending viruses or hacking programs that can destroy the victim's computer or delete personal information from their hard drive
- Posting intimate, sensitive and personal information about someone without their permission or knowledge

The above methods can also be used by adults to 'groom' vulnerable children and young people in order to sexually exploit them.
These people pretend to be someone else online in order to befriend a child or young person, find out sensitive information or obtain intimate photographs of them. They can then threaten to expose this information to their family of friends.

Published Content and the Fairfield School Web Site

The contact details on the Fairfield web site are the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

Photographing Pupils and Publishing Pupils' Images and Work on the Internet

Photographs which include pupils be appropriately selected with authorisation checked. Pupils' full names will not be used anywhere on the school website or particularly in association with photographs.
Written permission from parents/carers will be obtained before photographs of pupils are published on the school website.

Social Networking and Personal Publishing

The internet access provided by the LA will be set to filter access to inappropriate social networking sites, unless a specific use is approved. Staff must not access social networking sites for personal use via school information systems or using school equipment.
Newsgroups will be blocked unless a specific use is approved.
Pupils will be advised never to give out personal details of any kind which may identify them or their location.
Staff are advised not to communicate directly with parents or children using public social networking sites such as Facebook, My Space, Twitter, etc. For addition information please refer to the Social Media policy.

Managing Filtering

The school will work in partnership with the LA and ICT Services to ensure systems to protect pupils are reviewed and improved. Users will be informed that network and internet use will be monitored. Unsuitable material identified must be reported to the SLT / ICT Network Manager.

Authorising Internet Access

All staff will be directed to read the school Online Safety Policy and will be asked to read and sign the Acceptable Use Policy prior to accessing ICT resources. Visitors to the school who require access to a school networked computer will be given restricted access via a 'visitor' log-on. Instructions in safe and responsible internet use will be delivered regularly to pupils (where appropriate)

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date – always install the latest updates
- Staff members must not use the device in any way which would violate the school's terms of acceptable use policy

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, it is not always possible to guarantee that unsuitable material will never appear on a school computer. Fairfield School cannot 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 E-safety policy is effective.

Staff and the Online-Safety Policy

All staff will be asked to read and adhere to Fairfield School Online-Safety Policy (Parago). Our Online-Safety policy is reviewed annually. Staff should be aware that Internet traffic can be monitored and traced to the individual user in school. Discretion and professional conduct is essential at all times. All staff have a responsibility to adhere to the Online-Safety Policy, and to report any concerns to Jonathan Haigh or the SLT.

November 2021

Appendix 1

Fairfield School
Embracing Uniqueness

E-Safety Incident Report Log 2021 - 2022

Details of E-Safety incidents to be recorded by the SLT/DSL or ICT leads.
If an incident involves a pupil, a blue form will also need to be completed and passed onto DSL/DDSL
The incident Log will be monitored by the DSL or ICT Network Manager

Date	Name of student /staff	Time	Room / Device Number
Details of Incident	**Actions Taken**		**Outcome**

Date	Name of student /staff	Time	Room / Device Number
Details of Incident	**Actions Taken**		**Outcome**