Fairfield Endowed CE (c) Junior School

On-line Safety Policy

Introduction

We aim to provide a diverse, balanced and relevant approach to the use of technology. Children are encouraged to maximise the benefits and opportunities that technology has to offer and we aim to ensure that children learn in an environment where security measures are balanced appropriately with the need to learn effectively.

We aim to equip children with the skills and knowledge to use technology appropriately and responsibly and to recognise the risks associated with technology and how to deal with them, both within and outside the school environment. We aim to work with all members of the school community so there is a shared understanding for the need of an On-line Policy, which is regularly reviewed.

The school's E-safety Policy has been agreed by staff, discussed with the School Council and approved by governors. The E-Safety Policy and its implementation will be reviewed on an annual basis by the **Governing body's appropriate sub-committee**.

As a Rights Respecting School we ensure that children are made aware of Article 17 of the convention 'Children have the right to reliable information from the mass media. Television, radio, and newspapers should provide information that children can understand, and should not promote materials that could harm children.'

The ICT Co-ordinator will have responsibility for E-safety, supported by the Headteacher, Deputy Headteacher and PSHCE Coordinator. The current ICT Co-ordinator is **Mr Neil Redman.**

The aim of this policy is to protect the interests and safety of the whole school community.

Linked policies include: **Health and Safety; Child protection; Safeguarding; Behaviour; Anti-bullying; home–school agreements; ICT and PSHCE.**

Teaching and Learning

Why Internet use is important

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is an integral part of the curriculum and a useful tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

Internet use will enhance learning

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

- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils 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 what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Pupils will be taught how to evaluate Internet content

- 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 to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is a part of every subject.

E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote E-Safety.

- The school has a framework for teaching Internet skills as part of the ICT curriculum and E-safety is covered explicitly through computing sessions.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the E-Safety curriculum.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies: i.e.parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

E-Safety skills development for staff

- Staff receive regular information and training on E-Safety issues in the form of staff bulletins, INSET, staff meetings and staff induction.
- New staff members receive information on the school's acceptable use policy as part of their induction.

- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate E-Safety activities and awareness within all curriculum areas, where relevant.

Managing the school E-Safety messages

- We endeavour to embed E-Safety messages across the curriculum whenever the Internet and/or related technologies are used.
- The E-safety policy will be introduced to the pupils at the start of each school year.
- E-safety posters will be prominently displayed.
- The school uses E-Safety and Security software.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. Pupils are encouraged to login in and out of computers responsibly.

- All users read **and sign** an Acceptable Use Agreement to demonstrate that they have understood the school's E-safety Policy.
- Users are provided with year group login and individual passwords.
- Pupils are not allowed to deliberately access online materials or files on the school network, of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password report this to the ICT Coordinator.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platforms, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
- Due consideration should be given when logging into any systems to the browser/cache options (shared or private computer) to avoid unintentional access to others.
- ICT password policies are the responsibility of the E-Safety and ICT Coordinators and all staff and pupils are expected to comply with the policies at all times.

Managing Internet Access

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use is detected it will be followed up.

- Students will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile Internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastucture

- School Internet access is controlled through the LA's web filtering service.
- Fairfield Endowed CofE (C)Junior School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and Internet activity can be monitored and explored further if required.
- The school does not allow pupils access to Internet logs.
- If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the E-safety coordinator and Headteacher. The offending URL will reported to the LA.
- Anti-virus protections are provided by the LA [Microsoft Endpoint]and set to automatically update on all school machines.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the network manager and ICT Coordinator.

Managing other technologies

Various sites and systems (including the blogging site and other social networking sites) if used responsibly both outside and within an educational context, can provide easy to use creative, collaborative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to open access social networking sites to pupils within school (such as Facebook, WhatsApp, Instagram, snapchat].
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, Instant messenger/ email address, specific hobbies/ interests).
- Our pupils are advised to set and maintain profiles on any personal sites to maximum privacy and deny access to unknown individuals.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils are asked to report any incidents of bullying to the school immediately.
- Staff understand that it it is highly inappropriate to use open social networking sites (Facebook, WhatsApp, Instagram, snapchat), and public chat room facilities with pupils.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, and mobile phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible Internet access and thus open up risk and misuse associated with communication and Internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users access them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Only under exceptional circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device and this would be purely for professional reasons, for example, if parents need to be contacted while staff are supervising pupils off-site and the school office is closed.
- Technology may be used, for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Capturing images & video is not allowed by students / staff unless on school equipment and for educational purposes.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

E-mail

The use of email is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including: direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'.

- The school gives all staff their own Staff Mail account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Email sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending emails to external organisations, parents or pupils are advised to cc, (where appropriate) the Headteacher, line manager or designated account.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- All email users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/trusted adult if they receive an offensive message and keep the offending message(s) as evidence. This information must be passed to the E-Safety Coordinator and the headteacher.
- Staff must inform (the On-line Safety Coordinator) if they receive an offensive email.
- Pupils are introduced to email as part of the ICT Scheme of Work.
- Pupils may only use approved 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.
- The forwarding of chain letters is not permitted.

Published content and the school's Website

- The contact details on the website should be the school address, e-mail, telephone number and fax number. Staff or pupils' personal information will not be published.
- The headteacher will delegate editorial responsibility to individual staff with responsibility for their own class/subject/admin pages. All staff should ensure that content is accurate and appropriate.

- The school's website may be used to engage in collaborative projects with other school across the world within a protected environment after express agreement from Headteacher and ICT co-ordinator.

Publishing pupils' images and work

- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Photographs of pupils and pupils' work may be published on the website unless parents or carers request otherwise.
- With the written consent of parents the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of others, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupils device.

Related Issues

- It is assumed that staff give permission for their photos to be used unless they request in writing that they do not wish this to be the case.
- Parents are able to take photos of/ film school events such as sporting fixtures or class assemblies and are reminded that any images or recordings are not posted publically on the Internet.

Social networking and personal publishing

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

Managing filtering

- The school will work with the LA, DfES 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 ICT Co-ordinator immediately.

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

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to provide generic permission to use their child's work/photos in the following ways:

- on the school web site
- on the school's closed group (invitation only) social media platform eg. Facebook group.
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

Please refer to Parent Handbook for more details re permissions.

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time. Pupils' names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Storage of Images

- Images/ films of children can be stored on the school's network [to be deleted up to 2 years after leaving this school [to comply with GDPR regulations].
- Rights of access to this material are restricted to the staff and pupils within the confines of the school network/ Learning Platform

Managing videoconferencing

When essential to lessons or conducive to an enhanced ICT/ other curriculum lesson learning experience,

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' 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.
- Staff mobile phones will not be used during lessons or formal school time.
- Pupils are requested not to bring mobile phones into school. If mobiles are brought into school, they should be handed in to the school office and collected at the end of the day.
- The sending of abusive or inappropriate text messages is forbidden.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2016.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are denied Internet access.
- At Key Stage 2, Internet and e-mail access will be granted to a whole class as part of the ICT Scheme of Work, after a suitable education in responsible Internet use.
- Parents will be asked to sign and return a form if they do not wish their child to have independent internet access in Key Stage 2.

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. The school can not accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the E-Safety Coordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-Safety Coordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences
- Users are made aware of sanctions relating to the misuse or misconduct as part of the ICT induction lesson at the beginning of each school year (first lesson). Access rights will be removed for individuals who misuse access. Specific sites are available and vetted as part of the LA and school firewall settings.

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 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.

Community use of the Internet

- Community groups will be expected to work with the school to establish a common approach to E-safety.

Communications Policy

Introducing/Revisiting the E-safety policy to pupils

- E-safety rules will be posted in all networked rooms 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 prospectus and on the school Web site.
- Parental consent for Internet access and for Web publication of work and images will form part of the home-school agreement.
- An annual E-Safety workshop will be run for parents and the advice/information given will be available on the website.

Our school aims to support all families and the wider community. Any queries or concerns regarding individual policies will be considered on an individual basis.

Fairfield Endowed CE (c) Junior School

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 online-safety 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 role.
- Outside core teaching time, legitimate private interests may be followed, providing school use is not compromised. Social networking sites should never be accessed on school equipment.
- 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 that is not intended for educational purposes.
- 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 ICT Co-ordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety 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: …… Capitals: …… Date: ……

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