



Internet & E-Safety Policy

Folkestone St. Mary's C.E. Primary Academy believes in the educational benefits of curriculum internet use. The school management recognizes that there are risks and dangers associated with inappropriate use and so plans accordingly to ensure appropriate, effective and safe student and adult use.

Table of Contents:

E-Safety Audit	3
Letter to Parents	4
Introduction to the Policy	5
Publicising e-Safety	6
Roles and Responsibilities	6
Physical Environment/Security	6
Mobile/Emerging Technologies	7
Use of the Internet is Important	7
Internet Benefits for Education	7
How the Internet will Enhance Learning	7
Students will Learn to Evaluate Internet Content	7/8
Email	8
Published Content	8
Digital Media	8
Social Networking and Online Communication	8/9
Internet Access Records	9
The risks will be assessed	9
Management of Filtering	9
Dissemination of Rules	10
Staff Rules	10
Parental Support for E-Safety	10
Data Security/Data Protection	10
Wider Community	10
Responding to Incidents	10/11
Pupil ICT User Policy	11/12

E-Safety Audit

This rapid self-audit is used annually and helps the Senior Leadership Team (SLT) assess whether the e-safety basics are in place to support a range of activities that might include those detailed within the main E-Safety Policy

Has the Academy an E-Safety Policy that complies with CFE guidance?	Y
Date of latest update: September 2021	
The Policy was agreed by governors on:	
The Policy is available for teaching and non-teaching staff on the Academy Network/Website	
The Policy is available for governors and parents on the Academy website	
The Designated Safeguard Leads are: Trevor North and Kim Gardiner	
The E-Safety Co-ordinator is: Denise Judd	
The E-Safety Co-ordinator or a member of the Senior Leadership Team has received CEOP training	
Has e-safety training been provided for both students and all teaching and non-teaching staff?	Y
Have all staff seen and read a copy of the ICT policy?	Y
Do pupils when old enough, sign and return an agreement that they will comply with the Academy E-Safety rules?	Y
Have Academy E-Safety rules been set with consultation of students?	Y
Are these rules displayed in all rooms with computers?	Y
Internet access is provided by an approved educational internet service provider and complies with DfES requirements for safe and secure access (EIS at Kent Community Network)?	Y
An ICT security audit has been initiated by the ICT Team using some external expertise?	Y
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y

Dear Parent/Guardian

Responsible Internet and Computer Use Policy

As part of your child's curriculum and the development of ICT skills, Folkestone St. Mary's CEP Academy is providing access to the Internet. We believe that the effective use of the World Wide Web, including Web 2.0 and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please read the Internet and E-safety Policy on St. Mary's C.E.P. Academy website <http://www.stmarysfolkestone.com> in order to understand the terms and conditions of Internet and computer use at St. Mary's.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. St. Mary's C.E.P. Academy operates a filtering system that restricts access to inappropriate materials. This may not be the case at home, particularly with the rise in use of digital media. We therefore provide references to information on safe internet access on our Academy website, in our newsletters, at parents' meetings and particularly during World E-Safety week in February.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the Academy cannot be held responsible for the nature or content of materials accessed through the Internet. The Academy will not be liable for any damages arising from your child's use of the Internet facilities.

Should you wish to discuss any aspect of the Internet and E-safety Policy, please do not hesitate to contact (ICT Operations Manager).

Yours sincerely,

Trevor North
Principal

Introduction

The statutory curriculum requires students to learn how to locate, retrieve and exchange information using ICT and to ensure that they have an understanding of computer science for current and future learning. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.

Most technologies present risks as well as benefits. Internet use for work, home, social and leisure activities is expanding in all sectors of society. This brings young people into contact with a wide variety of influences, some of which – as in life generally – may be unsuitable. It is important that schools, libraries and youth clubs, as well as parents, adopt strategies for the safe and responsible use of the Internet.

Our Internet and E-Safety Policy has been written by the Academy, building on government guidance. It has been agreed by the Senior Leadership and approved by Governors. It will be reviewed annually.

Publicising E-Safety

Effective communication across the community is key to achieving the Academy vision for safe and responsible citizens. To achieve this we will:

- Make this policy and related documents, available on the Academy website at: <http://www.folkestonestmarys.com>.
- Introduce this policy and related documents to all stakeholders at appropriate times. This will be at least once a year or whenever it is updated. Post relevant e-safety information in all areas where computers are used.
- Provide e-safety information at parents' evenings, on the Academy website and through the Academy newsletter. Ensure all children receive ongoing internet safety education throughout the year.

Roles and Responsibilities

The Principal and Governors have ultimate responsibility for establishing safe practice and managing e-safety issues at our school. The role of the E-Safety Co-ordinator has been allocated to Denise Judd. She is the central point of contact for all e-safety.

All members of the Academy community have certain core responsibilities within and outside the Academy environment and are aware of e-safety issues. They should:

Use technology responsibly

Accept responsibility for their use of technology

Model best practice when using technology and remind pupils of e-safety issues

- Report any incidents to the E-Safety Co-ordinator using the Academy procedures
- Understand that network activity and online communications are monitored, including any personal and private communications made via the academy network
- Be aware that in certain circumstances, where unacceptable use is suspected, enhanced monitoring and procedures may come into action

Physical Environment/Security

The Academy endeavours to provide a safe environment for the whole community and we review both physical and network security regularly and monitor who has access to the system, consulting external advisers where appropriate.

- Anti-virus software is installed on all computers and updated regularly.
- Central filtering is provided by and managed by EIS (Kent). St. Mary's Academy can add further restrictions as required. All staff and students understand that, if an inappropriate site is discovered, it must be reported to the E-Safety Co-ordinator who will report it to the Academy ICT Consultant Network Manager to be blocked.
- All incidents will be recorded in the e-safety log for audit purposes, which is kept by the Safeguard Lead.
- Requests for changes to the filtering will be directed to the ICT Committee.
- The Academy uses monitoring software on all Academy owned equipment to ensure compliance with the Acceptable Use Policies.
- All staff are issued with their own username and password for network access. Visitors/supply staff are issued with temporary ID's and the details recorded in the school office.
- All pupils are issued with their own username. Passwords are being set for Y3 and Y4 pupils, whilst Y5 and Y6 will be taught how to create their own strong password. They need to understand that this must not be shared. The class teacher will keep a copy of these passwords. Supply teachers need to be informed where these are kept by the member of staff who inducts them.
- All teaching and non-teaching staff will have annual training of e-safety by a qualified e-safety advisor/trainer.
- Pupils will not be allowed to be on laptops unsupervised.
- Child protection and sensitive information is kept on a restricted area of the server, which is only accessible by the DSL Team.
-

Mobile/Emerging Technologies

- Teaching staff at the Academy are provided with a laptop for educational use and their own professional development. All staff understand that the Acceptable Use Policies apply to this equipment at all times. All staff shall sign an equipment loan form agreeing to keep the equipment safe at ALL times. They understand the equipment is loaned for the sole purpose of professional development in order to improve their expertise for the benefit of the children. They agree NOT to keep any sensitive data on the device regarding pupils.
- To ensure the security of the Academy systems, personal equipment is currently not permitted to be connected to the Academy network.
- Staff understand that they should use their own mobile phones sensibly and during non-contact time ONLY. They should not be used in class unless SLT permission has been granted.
- Mobile phones for pupils are only to be brought into school with parental permission. They should be handed in at the school office, who will keep them in a secure place until the pupil collects at the end of the day.
- The Education and Inspections Act 2006 grants the Principal the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Principal or deputies will exercise this right as appropriate.
- Pictures/videos of staff and pupils must not be taken on personal devices.
- New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the Academy community.

Use of the Internet is Important

- The purpose of internet use in our Academy is to raise educational standards, to promote student achievement, to promote the development of the children as lifelong learners in a continually developing technological world, to support the professional work of staff and to enhance the Academy's management information and business administration systems.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

Benefits of using the Internet in education include:

- Access to world-wide educational resources, including museums and art galleries.
- Inclusion in government initiatives such as the DfES ICT in Schools and the Naace ICT association (Naace) <http://www.naace.co.uk>.
- Educational and cultural exchanges between students world-wide.
- Cultural, vocational, social and leisure use in libraries, clubs and at home.
- Access to experts in many fields for students and staff.
- Staff professional development through access to national developments, educational materials and good curriculum practice.
- Communication with support services, professional associations and colleagues.
- Improved access to technical support including remote management of networks.
- Exchange of curriculum and administration data with the LEA and DfES.

How the Internet will Enhance Learning

- The Academy's internet access is designed expressly for educational use and will include 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.
- Staff should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.
- Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Students will Learn to Evaluate Internet Content

Academy staff model appropriate use of Academy resources including the internet.

- Where appropriate, especially at KS1 and Lower KS2, links to specific websites will be provided instead of open searching for information.

- Students will be taught how to conduct safe searches of the internet, using a variety of search engines and this information will be made available to parents and carers.
- E-safety will be embedded across the Academy curriculum.
- The e-safety program will be delivered throughout the year across all age groups.
- Teachers will be responsible for their own classroom management when using ICT equipment and will remind pupils of the Acceptable Use Policies before any activity.
- Staff, and when appropriate students, will be expected to reference third party resources that are used and will be taught the need to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- If staff or students discover unsuitable sites, the URL (website address) and content must be reported to a teacher who will then inform the E-Safety Technician.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

E-mail

The Academy email system is provided, filtered and monitored by Microsoft.

- All staff are given an Academy email address and understand that this must be used for all professional communication.
- All pupils have access to a class-based email account that is monitored by the class teacher and is used for class-based activities.
- Staff are allowed to access personal email accounts on the Academy system outside directed time and understand that any messages sent using the school equipment should be in line with the email policy.
- Everyone in the Academy community understands that any inappropriate emails must be reported to the Class Teacher/E-Safety Co-ordinator as soon as possible.

Published Content

The Principal takes responsibility for content published to the school website or facebook and carries out general editorial responsibility with the Webmaster. Class teachers and Phase Leaders are responsible for the editorial control of work published by their students.

- The Academy will hold the copyright for any material published on the school website or will obtain permission from the copyright holder prior to publishing with appropriate attribution.
- Anything published must be grammatically correct and accurate spelling throughout.
- The Academy encourages the use of email to contact the Academy via the Academy office/generic email addresses/staff email addresses.
- The Academy does not publish any contact details for the pupils.
- The Academy encourages appropriate, educational use of other Web 2.0 technologies (flash/meetings, Skype, Podcasts, eTwinning, blogs, online debates) and where possible embeds these in the Academy website or creates an Academy account on the site.

Digital Media

We respect the privacy of the Academy community and have the written permission from parents or carers before any images, podcasts or videos are published or distributed outside the Academy. Written permission is obtained from parents or carers when pupils first enter the Academy and this includes the use of video/conferencing in the Academy. Staff are asked for their permission when the need arises. Additional parental permission is sometimes required when pupils are publishing on BBC World Class, British Council or other similar sites:

- Photographs will be published in line with Naace guidance and not identify any individual pupil.
- Students' full names will not be published outside the Academy environment.
- Supervision of video conferencing (flash/meetings, Skype) will always be with a teacher, where the students will be directed by teachers to take part, full names of students should never be given in these.

Social Networking and Online Communication

The Academy is constantly reviewing the use of social networking sites and online communication and does not allow access to social media sites within the Academy.

Staff members are strongly advised NOT to add current or past pupils on social networking sites and be aware of friends of friends, the Academy will not take any responsibility from any matters arising from such sites.

The Academy will, however, take action in line with the disciplinary policy against staff, pupils, governors who bring the Academy into disrepute on social media sites.

Staff should not discuss/comment about the Academy on social sites and should act in a professional manner outside of the Academy.

Guidance is provided to the Academy community on how to use these sites safely and appropriately. This includes:

- not publishing personal information.
- not publishing information relating to the Academy community.
- how to set appropriate privacy settings.
- how to report issues or inappropriate content.
- un-moderated chat sites present an unacceptable level of risk and are blocked in the Academy. Pupils are given age appropriate advice and guidance around the use of such site.

Internet Access Records

- The Academy will keep a record of any students whose parents have specifically denied internet or email access.
- By using the internet, students are agreeing to abide by the Responsible Internet Use Statement, in line with the Pupil ICT Policy.

Risks will be Assessed

- In common with other media such as magazines, books and video, some material available via the internet is unsuitable for students. The Academy 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 an Academy computer. The Academy cannot accept liability for the material accessed, or any consequences of internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Management of Filtering

- The Academy will work in partnership with the LEA, DfES and the Internet Service Provider to ensure systems to protect students are regularly reviewed and improved.
- If staff or students discover unsuitable sites, the URL (address) and content must be reported to the E-Safety Co-ordinator.
- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- According to the **PREVENT** strategy and for safeguarding purposes, particular attention must be paid to ensure that pupils are safe from terrorist or extremist material when accessing the internet through the school system by establishing appropriate levels of filtering (see Safeguarding Policy).
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective, reasonable and appropriate.
- Any material that the Academy believes is illegal will be reported to appropriate agencies such as IWF, Kent Police or CEOP.
- Ad hoc checks are made to monitor internet site usage.

Dissemination of Rules

As part of the ICT curriculum, pupils will be taught the rules for safe and responsible use of the internet. Rules for internet access will be posted in all rooms where computers are used.

- Students will be informed that internet use will be monitored.
- Instruction/reminder in responsible and safe use will precede internet access.

Staff Rules

- All staff are governed by the terms of the 'Responsible Internet Use' in the Academy.
- All staff including teachers, supply staff, teaching assistants and support staff, will be provided with the Academy Internet and E-Safety Policy and its importance explained.
- Staff should be aware that discretion and professional conduct is essential. They should also be aware that the E-Safety Policy is an Academy Policy and it is a breach of professional standards if not adhered to.
- The monitoring of internet use is a sensitive matter. Staff who operate monitoring procedures are supervised by senior leadership.
- Staff development in safe and responsible internet use and on the Academy Internet Policy will be provided on a yearly basis.

Parental Support for E-Safety

- Parents' attention will be drawn to the Academy Internet and E-Safety Policy in parent meetings, assemblies, newsletters, the Academy prospectus and on the Academy website.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe internet use at home.
- Interested parents will be referred to organisations such as, NSPCC, ChildNet, ThinkuKnow, Kidsmart and CEOP.

Data Security/Data Protection

Personal data will be recorded, processed, transferred and made available in line with the Data Protection Act 1998. Sims, along with other sensitive Data is backed up remotely by Kent LEA.

Less sensitive data is backed up daily internally.

The Academy has a secure web based MIS system.

Wider Community

- Adult users will be provided with a copy of the Acceptable User Policy.
- Parents/carers of children will be required to sign an Acceptable Use Policy along with the signature of the child on the new Pupil ICT Policy.

Responding to Incidents

Inappropriate use of the Academy's resources will be dealt with in line with other Academy policies e.g. Behaviour, Anti-Bullying and Child Protection Policy.

- Any suspected illegal activity will be reported directly to the police.
- Third party complaints, or from parents concerning activity that occurs outside the normal Academy day, should be referred directly to the Principal.
- Breaches of this policy by staff will be investigated by the Principal. Incidents will be fully investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct.
- Student policy breaches relating to bullying, drugs misuse, abuse and suicide must be reported to the nominated child protection representative and action taken in line with Academy anti-bullying and child protection policies. There may be occasions when the police must be involved.
- Serious breaches of this policy by students will be treated as any other serious breach of conduct in line with the Academy Behaviour Policy. Referral to Leads of Key Stages may be appropriate at this level. For all serious breaches, the incident will be fully investigated, and appropriate records made on personal files with the ultimate sanction of exclusion reserved for the most serious of cases.

- Minor student offenses, such as being off-task visiting games or other websites will be handled by the teacher in situ by invoking the Academy Behaviour Policy.
- The Education and Inspections Act 2006 grants the Principal the legal power to take action against incidents affecting the Academy that occur outside the normal Academy day and this right will be exercised where it is considered appropriate

Notes on the Pupil ICT User Policy

This was reviewed with the School Council. The following requests were made by the Academy Council:

1. The Pupil ICT User Policy should be reviewed each year by the Academy Council, in order to keep abreast with the advance of mobile technology.
2. A large copy of the AUP should be displayed in classes
3. The AUP is signed by all pupils (age appropriate).

Folkestone St. Mary's C.E. Primary Academy Pupil ICT User Policy

Folkestone St Mary's C E Primary Academy recognises that ICT and the internet are integral parts of learning and the modern world. We understand that our children are digital natives and have grown up using this technology and expect them to use it safely and responsibly.

When using Computer Equipment in the Academy

- ✚ My behaviour on the internet will be monitored by the adults in the Academy.
- ✚ I will use Academy ICT for Academy purposes only.
- ✚ I will only access my own documents and user area unless explicitly told to do so by the adult in charge.
- ✚ I am responsible for actions which take place under my username and will ensure that my passwords are to be kept secure and never shared with another pupil.
- ✚ I will not bring in my own mobile technology unless otherwise directed by the Academy. I will use the systems in place for storing phones if I need to bring one into school.
- ✚ I will think carefully about the appropriateness of the things I am saving, downloading or sending to others.
- ✚ I will access only sites that have been approved by an adult
- ✚ Uploading and downloading of non-approved Apps will not be permitted.
- ✚ I will be careful and keep my personal information safe and not publish my address, telephone number or full name online nor will I arrange to meet anyone I have met online.
- ✚ I will only create images or recordings of people in appropriate situations when I have their permission or the permission of the adult in charge of the group
- ✚ I am aware of copyright (music, text and images) and plagiarism (copying from the internet or books) and will not intentionally claim the work of others as my own.
- ✚ I am aware that the information given on internet sites is not always accurate.
- ✚ I will be responsible for my behaviour when using ICT because I know these rules are designed to keep me safe. I understand that the above rules will also keep me safe when using the internet at home.
- ✚ When using technology to communicate, I will be respectful and remember not to say anything that I would not say directly to them in person.
- ✚ I will report any inappropriate images or text that I see or have been sent to an adult

If I break these rules or staff have concerns about my E-Safety:

- ✚ The incident will be logged and investigated.
- ✚ My parent/carer will be contacted.
- ✚ I will receive consequences from the Academy's Behaviour Policy and could result in withdrawal of IT and internet use within the Academy.

I have read and understood these rules and promise to abide by them

Name: _____

Signed: _____ Date _____