



Eaton Square School

C5. Online Safety and Security Policy **Eaton Square School Online Safety and Security Policy 2022**

This policy is for the whole school, including EYFS

Reviewed: Tomasz Magiera – IT Consultant/Data Manager	4.9.22
Approved by: Mrs Trish Watt Headmistress	07.09.22
Next review: September 2023	

The School has written our own Acceptable Use Policy, building on the BECTA policy and government guidance. It has been agreed by the Senior Management Team. It will be reviewed annually. This Policy can also be found in the School Handbook.

Aims

1. To allow all users to access and use the Internet for educational purposes. This can include email and World Wide Web facilities. The school activities can cover individual research/preparation for lessons/project work/homework assignments/ communicating with other teachers and students.
2. Provide a mechanism by which staff and students are protected from sites, information and individuals, which would undermine the principles and aims of the School.
3. Provide rules which are consistent, and in agreement with the Data Protection Act.
4. Provide rules that are consistent with the acceptable use procedures commonly used on the Internet, including those associated with netiquette.

Why is Internet use important?

The purpose of Internet 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 information and business administration systems.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet access is an entitlement for students who show a responsible and mature approach to its use.

The Internet is an essential element in the 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

How will Internet use enhance learning?

Pupils 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. Access levels will be reviewed to reflect the curriculum requirements and age of the pupils. Staff should guide pupils in online 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.

How will email be managed?

Eaton Square School encourages the use of email as an essential means of communication for both staff and pupils. Directed email can bring significant educational benefits and interesting projects between our school, and ones in other parts of the world can be beneficial.

At Eaton Square School, the staff use email to disseminate information, memos and general notices. In this respect, school email accounts should not be considered private and 'the School' has the right to monitor emails. We aim to achieve a balance between monitoring as necessary to maintain the safety of pupils and the preservation of human rights. Monitoring of email accounts would occur only in extreme cases where the Headmistress or Principal was concerned about the inappropriate use of the School name or content.

Pupils are taught to email from Year 3 upwards. They are all allocated an individual email account, which is based on their first initial, surname and school domain.

For example:

j.Smith@eatonsquareschools.com

Using this procedure, students maintain their anonymity outside the School.

All student email accounts from Years 3-6 have very strict restrictions attached. Year 2 have a whole class account.

- For all students the banned word threshold is 0, meaning that no inappropriate words can be used in any emails at all.
- Pupils in Years 3-5 are only allowed to email in class with teacher supervision.
- Pupils in Years 6 are also restricted to the eatonsquareschools.com. domain, but can have restrictions lifted in individual cases by the Head of ICT only. In this age group, pupils are taught how to access their email accounts from home and are encouraged to email their work/homework etc into their teachers.
- Pupils must immediately tell a teacher if they receive offensive email; this includes emails containing bullying in any form.

At all stages, the pupils are taught:

- the correct use of passwords and the importance of keeping them secret;
- appropriate use of language, formatting, formality and informality (depending on the purpose of the email)
- Internet and email safety – not giving out any personal information, such as address or telephone numbers, at any time to anyone; not arranging to meet anyone via email.

Pupils and staff are aware that emails can be monitored at any time if there is cause for concern. If necessary, the Head of ICT will monitor pupil emails and the Headmistress or Principal will monitor staff emails.

Email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

The forwarding of chain letters is not permitted.

In a case where a pupil has sent an inappropriate email, the Headmistress will decide on the course of action. In some cases this may include suspension.

In a case where a staff member has sent an inappropriate email, the Headmistress will decide on the course of action as set out in the Contracts of Employment.

Staff should not use personal email accounts during lesson times; access could be restricted if this occurs.

How should website content be managed?

- The point of contact on the Website should be the School address, School email and telephone number. Staff or pupils' home information will not be published.
- Website 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 website, particularly in association with photographs.
- Written permission from parents will be obtained before photographs of pupils are published on the school website. Please see parent consent form.
- The Director of Marketing will take overall editorial responsibility and ensure that content is accurate and appropriate.

Social Networking

Introduction

Social networking activities conducted online outside work, such as blogging (writing personal journals to publicly accessible internet pages), involvement in social networking sites such as Facebook, Myspace or Bebo and posting material, images or comments on sites such as You Tube can have a negative effect on an organisation's reputation or image. In addition, Eaton Square School has a firm commitment to safeguarding children in all aspects of its work. This policy has been written to set out the key principles and code of conduct that we expect of all members of staff with respect to their responsibilities in connection with the use of social networking sites.

Key Principles

Everyone* at Eaton Square has a responsibility to ensure that they protect the reputation of the school, and to treat colleagues and members of the school with professionalism and respect.

*In the context of this policy "everyone" refers to members of staff, directors, Friends and anyone working in a voluntary capacity at the school

It is important to protect everyone* at Eaton Square from allegations and misinterpretations which can arise from the use of social networking sites.

Safeguarding children is a key responsibility of all members of staff and it is essential that everyone* at Eaton Square considers this and acts responsibly if they are using social networking sites out of school. Anyone working in the school either as a paid employee or volunteer must not communicate with children via social networking.

This policy relates to social networking outside work. Blogging and accessing social networking sites at work using school equipment is not permitted.

This policy is not covered by the Chatham House rule and therefore no communications irrespective of their anonymity should be shared that relate to any specific event, protocol, pupil or person at Eaton Square School.

Aims

To set out the key principles and code of conduct expected of all members of staff, directors, Friends and volunteers at Eaton Square School with respect to social networking.

To further safeguard and protect children and staff.

Code of Conduct for Everyone* at Eaton Square – Social Networking

The following are **not considered acceptable** at Eaton Square School:

The use of the school's name, logo, or any other published material without written prior permission from the Headmistress. This applies to any published material including the internet or written documentation.

The posting of any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.

The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.

The posting of any images of employees, children, directors or anyone directly connected with the school whilst engaged in school activities.

In addition to the above everyone* at Eaton Square School must ensure that they:

Do not make any derogatory, defamatory, rude, threatening or inappropriate comments about the school, or anyone at or connected with the school.

Use social networking sites responsibly and ensure that neither their personal/professional reputation, or the school's reputation is compromised by inappropriate postings.

Are aware of the potential of on-line identity fraud and to be cautious when giving out personal information about themselves which may compromise their personal safety and security.

Potential and Actual Breaches of the Code of Conduct

In instances where there has been a breach of the above Code of Conduct, the following will apply:

Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the Disciplinary Procedure. A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the school's ethos and principles.

The Directors will take appropriate action in order to protect the school's reputation and that of its staff, parents, children and anyone else directly linked to the school.

How will Internet access be authorised?

Eaton Square School allocate Internet access to staff and pupils based on education need. All Internet usage by pupils is fully supervised at all times.

- Pupils in Key Stage 1 and Year 3 are restricted to using approved sites which have links provided by the teachers. Any general searching is very strictly monitored and at no time are the pupils allowed to search freely.
- In Years 4, 5 and 6, pupils can begin using approved search engines, under strict supervision, on their Microsoft Surface Go devices. They are taught to evaluate all content and to respect copyright regulations. The School's firewall has strict blocks in place, to limit the risk of children accessing websites with

inappropriate content. Teachers can also monitor the student's devices through 'Classwize', allowing them to view the children's screens from their own device and block certain websites.

How will the risks be assessed?

'In common with other media such as magazines, books and videos, some material available via the Internet is unsuitable for pupils. 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. Eaton Square School 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.

http://www.legislation.hmso.gov.uk/acts/acts1990/ukpga_19900018_en_1.htm

Methods to identify, assess and minimise risks will be reviewed regularly. The Headmistress will ensure that the Internet Policy is implemented and compliance with the policy monitored.

How will filtering be managed?

The School will ensure systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Head of ICT who will report it to the Filtering Provider.

Any material that the school believes is illegal will be referred to the Internet Watch Foundation (www.iwf.org.uk).

The School, in discussion with the filtering provider, will select filtering strategies where appropriate. The filtering strategy will be selected to suit the age and curriculum requirements of the pupils.

How will the policy be introduced to the pupils?

Many pupils are familiar with Internet use and culture. Pupils' perceptions of the risks involved will vary so rules will need to be explained and discussed. Pupils may need to be reminded of the School rules at the point of Internet use by referring to the Acceptable Internet and Computer Use Rules, (Appendix C5b). These rules are displayed in all rooms where computers are used. A copy of the pupils' rules will be given to parents.

Pupils and staff will be informed that Internet use can be monitored and will be if necessary.

How will the staff be consulted?

It is important that teachers, learning support assistants, teaching assistants and administration staff are confident to use the Internet in their work. Staff should be given the opportunity to discuss issues and develop appropriate teaching strategies.

All staff must read the terms of the 'Acceptable Internet and Computer Use' statement, (Appendix C5a) before using any Internet or computer resource in school.

Staff must be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Staff and pupils must understand the importance of maintaining security on the network. In this respect, staff and pupils must **always** log on under their own username, and at the end of a session must **always** log off.

No one is allowed access to another people's files unless given specific permission.

Staff should not knowingly delete any files other than their own. Deliberately deleting files belonging to the School or other individual teachers can result in action based on the Computer Misuse Act 1990.

How will the ICT system be managed?

The whole system will be checked regularly for any security risks. The Head of ICT will do this on a basic level, with occasional checks on user files, temporary Internet files and history files. A more thorough check can be done by the ICT Support Company – Compatibility.

- The School ICT systems will be reviewed regularly with regard to security.
- Virus protection is installed and updated on a weekly basis.
- Use of portable media such as floppy disks, memory pens and CD ROMs will be reviewed. Portable media may not be brought into school without specific permission and a virus check.
- Files held on the School's network will be regularly checked.
- Users must act reasonably. Loading non-approved software could cause major problems. All questions about software, including floppy disks, CD ROMS and DVDs must be directed to the Head of ICT or Compatibility.
- Good password practice is required including logout after use.

How will complaints about Internet/computer use be handled?

A clear process is in place to handle complaints about Internet or computer use.

Staff Misuse

A complaint about staff misuse may be referred to the Headmistress.

Staff misuse can include, although is not exclusive to:

- Leaving a computer logged on after use.
- Accessing inappropriate websites.
- Accessing restricted files on the network.
- Deleting or altering other people's files without permission.
- Sending emails from the staff member's school account with inappropriate/illegal content.

If an incident has been reported to the Headmistress, a variety of actions can take place as explained in the Staff Contract of Employment.

Pupil Misuse

A complaint about pupil misuse will be referred to the Head of ICT as a first response. If it needs to be dealt with further, it will be referred to the Heads of Department or Deputy Head, and if necessary, the Headmistress. Parents will be contacted if the Headmistress deems it necessary.

Pupil misuse can include, although is not exclusive to:

- Accessing the Internet without teacher permission and supervision
- Sending inappropriate emails
- Deliberately deleting files belonging to other pupils or teachers

If an incident has been reported to the Head of ICT, a variety of actions can take place based on the clearly established Behaviour Management Policy.

- The class teacher as part of the normal class discipline can deal with a minor transgression of the rules.
- Interview/counsel by the Head of ICT with a warning given.
- Informing parents.
- Referring to the Headmistress or other senior management.
- Removal of computer/Internet access for a period, which could ultimately prevent access to files to complete school work.
- In extreme cases, a pupil can be suspended for a period of time determined by the Headmistress.

How will parents' support be enlisted?

Parents attention will be drawn to the School's Acceptable Use Policy in newsletters and the School website. A copy of the policy will be sent home annually when the parents are asked to sign the parents consent form.

It is important that parents are aware of the dangers of unrestricted access to the Internet and ways they can help their child at home. Internet issues must be handled sensitively to inform parents without undue alarm.

We encourage a partnership with parents. Suggestions are made to parents for safe Internet use at home. We aim to promote a consistent approach between the home and school.