Mayflower Community Academy

Internet and Email Policy

VERSION CONTROL SHEET

POLICY NAME: Internet and Email Policy

Policy Prepared by: Nigel Gooding

Document date	Filename	Meeting submitted	Summary of changes required
01-09-13		July PSG	New policy
11-10-19		Nov LGB	Reviewed and updated
March 2021		19.03.21 LGB	Updated (no changes)

1. Core Principles of Internet Safety

The Internet has become as commonplace as the telephone or TV and its effective use is an essential life-skill. Unmediated Internet access brings with it the possibility of placing of pupils in embarrassing, inappropriate and even dangerous situations. Schools need a policy to help to ensure responsible use and the safety of pupils.

The Mayflower Community Academy Internet Policy is built on the following five core principles:

i. Guided educational use:

Significant educational benefits should result from curriculum Internet use including access to information from around the world and the abilities to communicate widely and to publish easily. Curriculum Internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful Internet use will also reduce the opportunities for activities of dubious worth.

ii. Risk assessment:

21st century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time, they must learn to recognise and avoid these risks – to become "Internet Wise". Schools need to ensure that they are fully aware of the risks, perform risk assessments and implement a policy for Internet use. Pupils need to know how to cope if they come across inappropriate material. Pupils may obtain Internet access in youth clubs, libraries, and public access points and in homes. Ideally a similar approach to risk assessment and Internet safety would be taken in all these locations, although risks do vary with the situation.

iii. Responsibility:

Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies such as phones. The balance between educating pupils to take a responsible approach and the use of regulation and technical solutions must be judged carefully.

iv. Regulation:

The use of a finite and expensive resource, which brings with it the possibility of misuse, requires regulation. For instance, un-moderated chat rooms present immediate dangers and are banned. Fair rules, clarified by discussion and prominently displayed at the point of access help pupils make responsible decisions.

v. Appropriate strategies

This document describes strategies to help to ensure responsible and safe use.
They are based on limiting access, developing responsibility and on guiding pupils towards educational activities. Strategies must be selected to suit the school situation and their effectiveness monitored. There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

The acceptable use policy affects all users. It is therefore important that all users of Mayflower Community Academy are aware of the policy. The E safety SWGFL reference pack is used in

conjunction with the schools existing Internet Policy. The section titled 'Safety and Security' compliments this existing policy and will be used as a point of reference and will be kept with all other documentation in the library with the ICT subject box.

2. Acceptable Internet Use at Mayflower Community Academy

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, wellbeing and 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 pupils who show a responsible and mature approach to its use.
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.

Benefits of using the Internet in education include:

1. access to world-wide educational resources including museums and art galleries
2. inclusion in government initiatives such as the DfE ICT in Schools and the Virtual Teacher Centre (VTC)
3. educational and cultural exchanges between pupils world-wide
4. cultural, vocational, social and leisure use in libraries, clubs and at home
5. access to experts in many fields for pupils and staff
6. staff professional development through access to national developments
7. educational materials and good curriculum practice
8. communication with support services, professional associations and colleagues
9. improved access to technical support including remote management of networks
10. exchange of curriculum and administration data with the LEA and DfE
11. mentoring of pupils and provide peer support for them and teachers

Developing good practice in Internet use

1. The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
2. Pupils will learn appropriate Internet use, what is and what is not appropriate use, and given clear objectives for Internet use.
3. Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
4. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Ideally inappropriate material would not be visible to pupils using the web, but this is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable, or threatening. For example: to close the page and report the URL to the teacher or ICT manager for inclusion in the list of blocked sites.

1. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Southwest Grid for Learning: 0870 9081708 or email: abuse@swgfl.org.uk via the ICT co-ordinator.
2. Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
3. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

3. E-mail

Restriction of incoming and outgoing e-mail to approved addresses and filtering for unsuitable content and viruses is now possible. This is a feature of Easy Mail+, which is available to the school, via the Southwest Grid for Learning (SWGfL). In the school context e-mail should not be considered private and most schools, and indeed firms, reserve the right to monitor e-mail.

There is a balance to be achieved between monitoring that is necessary to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

1. Pupils may only use approved e-mail accounts on the school system.
2. Pupils must immediately tell a teacher if they receive offensive e-mail.
3. Pupils must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.
4. Pupils should use email in an acceptable way as outlined in the SWGfL e-safety Policy.
5. Access in school to external personal e-mail accounts will be blocked.
6. Excessive social e-mail use can interfere with learning and may be restricted.
7. E-mail 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.
8. The forwarding of chain letters is not permitted.
9. Pupils will not be allowed access to public or unregulated chat rooms.
10. Children should use only regulated chat environments. This use will be supervised and the importance of chat room safety emphasised.
11. A risk assessment will be carried out before pupils are allowed to use a new technology in school.
12. Emerging technologies will be examined for educational benefit and a risk assessment will carried out before use in school is allowed

4. On-line Communications and Social Networking.

A number of technologies allow people to communicate other than by using; e-mail, Chat through the Microsoft service, such as Messenger allows pupils to send text messages, voice and web cam video in real time. There is also a range of newer services within the genre of Social Networking Sites that allow people to upload text, images, sound and video which can then be shared across the whole Internet, or with specific friends; examples include Facebook and Twitter. The ability to post personal information and communicate with friends is hugely appealing to young people, with an increasing number of Key Stage 2 pupils having accessed these services. It is a major concern how pupils use these appropriately and safely. For example, to ensure that only very limited personal information is included on a person's social networking site, not allowing them to be easily identified. All of these services and ones similar in nature are filtered by SWGfL. These are banned from pupil access while at school but are likely to be accessible from home. Schools have a key role to teach young people about the importance of keeping personal information safe, not posting comments and pictures of other

people that may cause upset and to communicate in an appropriate manner.

- Students / pupils will be taught about how to keep personal information safe when using online services. Each year group will have specific ICT lessons dedicated to e-safety. In accordance with SWGfL e-safety policy
- The use of online chat is not permitted in school, other than as part of any subscribed online learning environment. (VLE)

5. Internet Access

Internet access for pupils should be seen as an entitlement on the basis of educational need and an essential resource for staff. It should be clear who has Internet access and who has not. Parental permission will be required in all cases.

1. The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up to date, for instance a member of staff may leave, or a pupil's access be withdrawn.
2. At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
3. Parents will be informed that pupils will be provided with supervised Internet access
4. Parents will be asked to sign and return a consent form
5. Primary pupils will not be issued individual email accounts but will be authorised to us a group/class email address under supervision.

Risk Assessment

In common with other media such as magazines, books and video, 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. Neither the school nor Academy Trust can 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.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Headteacher will ensure that the Internet policy is implemented and compliance with the policy monitored.

Filter Management

Levels of access and supervision will vary according to the pupil's age and experience.
Internet access must be appropriate for all members of the school community from youngest pupil to staff.

The Academy will continue working with Plymouth LA in conjunction with the SWGfL have implemented Safety Net+. This service filters Internet access by cross referencing all web site requests against a banned list which is continually updated. In addition to this schools can permit or deny sites that they feel appropriate for the duration they choose.

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content.

Careful monitoring and management of the Internet filtering system will still be required, i.e., checking to ensure that staff are aware of this service and being proactive in its use. It is important that the school establishes the filtering criteria rather than simply accepting filtering default settings.

1. The school will work in partnership with parents, the Department for Children and Education or Plymouth City Council, DfE and the SWGfL to ensure systems to protect pupils are reviewed and improved.
2. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator.
3. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective, and reasonable.
4. Any material that the school believes is illegal must be referred to the Internet Watch Foundation (please see references given later).
5. Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate. The filtering strategy will be selected to suit the age and curriculum requirements of the pupil.

APPENDIX A

Responsible Internet use policy

Pupils:
Rules for Internet access will be posted in all rooms where computers are used.
Pupils will be informed that Internet use will be monitored.
Instruction in responsible and safe use should precede Internet access.

Staff:
All staff must accept the terms of the 'Acceptable Internet Use' statement before using any Internet resource in school.
All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained.
Staff should be aware that Internet traffic is monitored and reported by the SWGfL and can be traced to the individual user. Discretion and professional conduct are essential.
The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management.
Staff development in safe and responsible Internet use and on the school Internet policy will be provided as required.

Maintaining ICT Security:
The school ICT systems will be reviewed regularly with regard to security.
Virus protection will be installed and updated regularly, daily if possible (this can be achieved by using the self-updating feature within Sophos).
Security strategies will be discussed with the LEA, particularly where a wide area wireless network connection is being planned.
Personal data sent over the Internet will be encrypted or otherwise secured.
Use of portable media such as memory sticks and tablets will be reviewed.
Portable media may not be brought into school without specific permission and a virus check.
Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
Files held on the school's network will be regularly checked.

The IT co-ordinator / network manager will monitor the Internet usage and associated traffic in order to assess whether the capacity of the Internet is being reached.

Reporting incidents:
Parents and teachers must report all incidents to the Head Teacher. Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the Internet use was within or outside school. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's behaviour policy. Complaints of a child protection nature must be dealt with in accordance with the Academy's child protection procedures.

Responsible Internet Use - Pupils

These rules help us to be fair to others and keep everyone safe.

- I will ask permission before using the Internet.
- I will use only my class network login and password, which is secret.
- I will only open or delete my own files.
- I understand that I must not bring into school and use software or files without permission.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- I understand that I must never give my home address or phone number or arrange to meet someone.
- I will ask for permission before opening an e-mail or an email attachment sent by someone I do not know.
- I will not use Internet chat.
- If I see anything I am unhappy with or receive messages I do not like, I will tell a teacher immediately.
- I understand that the school may check my computer files, emails I send and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

The school may exercise its right to monitor the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.