Marist Brothers
Na Bráithre Muiristeacha

Phone: 4574837
Fax: 4577682
E.mail:
info@moyleparkcollege.ie
Website:
www.moyleparkcollege.ie

MOYLE PARK COLLEGE, CLONDALKIN, DUBLIN 22.
COLÁISTE PHÁIRC MHAOILE, CLUAIN DOLCÁIN, BAILE ÁTHA CLIATH.

MOYLE PARK COLLEGE ACCEPTABLE USE POLICY FOR INTERNET ACCESS FOR STAFF AND STUDENTS

Terms and Conditions

Moyle Park College is pleased to offer its users access to the Network and Internet for educational purposes. The use of the Network is important to prepare students for life and work in the 21st Century. College users are expected to follow all guidelines listed below.

- *Inappropriate use of the Network may result in a cancellation of access, in whole or in part.*
- *Such behavior will be reported to any relevant authorities*
- *Unacceptable use will be dealt with under the College Code of Behaviour, covering sanctions up to and including suspension or expulsion.*

Purpose

The purpose of this Policy is to ensure that:

- Everyone is informed about the policies relating to computer use, electronic mail and Internet access;
- Computers, Electronic mail and Internet services are used in compliance with this policy;
- Users of electronic mail services are informed about how concepts of privacy and security apply to electronic mail;
- Disruptions to School computer facilities and other services and activities are minimised.
- Users log on and use their own passwords which they do not disclose to any other person, be they be a member of staff or otherwise.

Important Notifications

- **No employee or student should have any expectation of privacy as to his or her Internet usage.** School Authorities can review Internet activity and analyze usage patterns to ensure Internet resources are devoted to maintaining the highest levels of productivity.

- School Authorities reserve the right to inspect any and all files stored in private areas of our network in order to assure compliance with policy.

- Filtering software and/or equivalent systems will be used in order to minimize the risk of exposure to inappropriate material.

- School internet accounts, must be secured by changing the generic password as soon as possible after the account is opened for a user. Any inappropriate use of that account will be the responsibility of the account owner.

Internet Chat

- Students should only access chat rooms, discussion forums, messaging or other electronic communication fora that have been approved by the school.
- Chat rooms, discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.
- Usernames will be used to avoid disclosure of identity.
- Face-to-face meetings with someone, organised via Internet chat will be forbidden.

School Website

- Pupils will be given the opportunity to publish projects, artwork or school work on the World Wide Web in accordance with clear policies and approval processes regarding the content that can be loaded to the school's website
- The website will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff.
- Website using facilities such as guestbooks, noticeboards or weblogs can be checked to ensure that they do not contain personal details.
- The publication of student work will be co-ordinated by a teacher.
- Pupils' work will appear in an educational context on Web pages with a copyright notice prohibiting the copying of such work without express written permission.
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Content focusing on individual students will not be published on the school website without parental permission.
- Personal pupil information including home address and contact details will be omitted from school web pages.
- The school will ensure that the image files are appropriately named – will not use pupils' names in image file names or ALT tags if published on the web.
- Pupils will continue to own the copyright on any work published.

Personal Devices

- Pupils using their own technology in school, such as leaving a mobile phone turned on or using it in class, sending nuisance text messages, or the unauthorized taking of images with a mobile phone camera (still or moving) is in direct breach of the school's acceptable use policy, unless done with the express permission of school authorities. Such breaches will be dealt with under the code of discipline.

Acceptable Uses:

The Network is to be used for educational purposes. The following types of access are considered to be appropriate uses:

1. To collaborate with other students in educational tasks.
2. To access real-time data of an educational nature.
3. To access unique resources.
4. To publish information and resources.
5. To conduct research.
6. To communicate broadly and effectively.

Unacceptable Uses;

The following types of access are considered to be inappropriate uses (the list is not exhaustive):

1. Accessing profane or obscene material, material suggesting illegal acts and material advocating violence or discrimination.
2. Using the access for illegal acts.
3. Attempts to access any resources that are restricted, confidential or privileged.
4. Posting chain letters.
5. Internet Relay Chat, news groups, or mailing list participation unless directed and supervised by a staff member for a classroom assignment.
6. Granting Internet or Network access to unauthorized persons intentionally or unintentionally, or failing to notify a teacher or administrator if you suspect someone of using your password.
7. Posting personal contact information.
8. Agreeing to meet someone met online without parental approval and under the supervision of a teacher or authorized adult.
9. Attempts to disrupt access.
10. Causing damage to or changing function, operation or design of the technology.
11. Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening language and/or images.
12. Harassing or insulting another person.
13. Posting false or defamatory information or images.
14. Using information found on the Internet as your own.
15. Breaking Copyright rules.
16. Uploading or downloading information that is copyrighted or owned by others.
17. Posting web pages without the permission of a teacher or authorized adult.
18. Downloading large files (over 5 MB) without permission.
19. Buying or selling any products or services not related to the school or services provided by the school.
20. Students or staff accepting/opening attachments that are not necessary for the school or services provided by the school.
21. The use of school facilities knowingly to download or distribute pirated software or data.
22. The use of the school's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.
23. The use of the school's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.
24. The Use of the college name on the internet in any unacceptable way.
25. Commenting about other school community members in any unacceptable way.

Storage media

No storage media should not be used with school IT resources without the media first being checked for virus contamination, malware, or programmes that would in any way harm the School infrastructure or equipment (including software).

Use of social media in the wider school community

• Be aware of what you post online. Social media venues including wikis, blogs, twitter, photo and video sharing sites are very public. What you contribute leaves a digital footprint for all to see. Do not post anything you wouldn't want friends, enemies, parents, teachers, or a future employer to see.

• Follow the school's code of conduct when writing online. It is acceptable to disagree with someone else's opinions, however, do it in a respectful way. Make sure that criticism is constructive and not hurtful. What is inappropriate in the classroom is inappropriate online.

- If you run across inappropriate material that makes you feel uncomfortable, or is not respectful, tell your teacher right away.

- How you represent yourself online is an extension of yourself. Do not misrepresent yourself by using someone else's identity.

- Be safe online. Never give out personal information, including, but not limited to, last names, phone numbers, addresses, exact birthdates, and pictures. Do not share your password with anyone besides your teachers and parents.

Representation

- Electronic mail users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the School or any unit of the School unless appropriately authorised (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing the School. An appropriate disclaimer is: "These statements are my own, not those of Moyle Park College."

Sanctions

- Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.
- This policy should be read in conjunction with the School Bullying Statement, Anti-Racism Statement, the Code of Behaviour, IT Policy and the Social Media Policy.

Signed: Chairperson of the BOM: Principal:
        Date: Date: