



OAKLANDS COMMUNITY COLLEGE

Social Media Policy

Mission Statement

As members of a caring school community, we promote respect for ourselves, each other and the school environment in a spirit of partnership and teamwork.

We are an inclusive school, committed to developing a culture of achievement where we nurture the full academic and personal development of all students in a safe and challenging learning environment. We aim to prepare all our students for the responsibilities and experiences of life.

CONTENTS

1. RATIONALE.
2. RELATION TO MISSION.
3. AIMS OF THE POLICY.
4. POLICY CONTENT.
5. ROLES AND RESPONSIBILITIES.
6. REVIEW AND EVALUATION.
7. APPENDICES

RATIONALE

There can be little doubt that we currently live in an information age where the majority of the content (photographs, music, video, print) we consume and create is of a digital nature. The distribution and sharing of such material on the Internet via Social Media sites such as Facebook, Twitter, MySpace, YouTube, Google+ etc. has become a feature of our times. Young people are now said to be 'digital natives' as the creation and sharing of content comes naturally to them.

Unfortunately there is scope for irresponsible and inappropriate use of Social Media sites and this can lead to bullying, harassment and illegal activity whilst online. We therefore need a policy to ensure the safe & responsible use of Social Media by all members of the school/centre community. This is necessary in order to protect students, staff and the good name of our school/centre.

AIMS

This Policy aims to:

- Produce a set of strategies for students that will allow them to use Social Media safely and responsibly.
- Protect the integrity and good name of all members of the school/centre community from online abuse.
- Outline behaviours which are unacceptable and the consequences for these.
- Provide guidance for staff on the appropriate use of Social Media.

POLICY CONTENT

1. Strategies to be taught to students to enable safe & responsible use of Social Media.

Use strict privacy settings.

Review all of the options on your privacy settings page. Many sites default settings tend to keep information public until a user makes it private (although Facebook is a little stricter with minors' accounts). "Friends Only" is a good choice for most items, but you can be even more selective.

Be selective and control what you post.

Be selective about what you share by customizing the recipients of your posts. Activities on Facebook, including the applications teens use and games they play, can be viewed by others. Remember: Everything online happens in front of a vast, invisible, and often anonymous audience. Once something is out there, it doesn't go away as it can be copied and forwarded easily and quickly. Everything leaves a digital footprint.

As a rule of thumb if you wouldn't be comfortable posting something (pictures comments etc.) on a noticeboard in the school corridor then don't post it online.

You should never post personal details such as your phone number, email address or home address.

Remember that irresponsible online behaviour can damage your real life reputation.

Be selective with friends.

Be careful who you make friends with online. In general it is better to restrict friends to people you know and trust in the real world.

Pre-approve tags.

Choose the settings that allow you to see everything you've been tagged in (including photos) before the tag links to your page.

Use notification settings.

You can tell Facebook that you want to be notified of any activity performed on your name, including photo tags.

Never post your location.

Facebook lets users post their location on every post. Teens should not do this for safety and privacy reasons. Teens can also "tag" their friends' location but you can prevent anyone from tagging your location in the How Tags Work section.

If something has been posted that upsets you – tell someone.

If someone is bullying you online, you should:

- As in all cases of repeated unwanted aggression you should tell your Class Tutor, Year Head, the Deputy Principal or Principal or any Teacher in the school.
- Keep and save any bullying emails or images you have been sent.
- Take a screenshot of any comments that are threatening.
- Make a note of the time and date that messages or images were sent, along with any details you have about the sender.
- Not reply to any bullying messages or get into any online arguments.

Using Social Media on your Mobile Phone.

If your profile is linked to your mobile phone, you should use the website's privacy settings to ensure that your phone number is not visible.

Chat & VOIP services. (These allow for communication that may be typed or spoken with or without webcam access)

When using the above you should only communicate with people you trust and remember that other people may be able to view all aspects of the communication.

Watch the clock.

Social media sites can be real time wasters. Hours and hours can go by online - time that should be spent doing homework, studying, reading or exercising.

Appendix A contains links to some online resources that may be useful in dealing with the above subject in class.

Appendix B contains information on reporting inappropriate use on the Facebook site.

2. Unacceptable uses of Social Media sites and their consequences.

Unacceptable use of Social Media sites will include:

- Sending or posting discriminatory, harassing, or threatening messages or images that may cause harm to any member of the school community.
- Forwarding or 'Liking' material that is likely to cause offence or hurt to a third party.
- Sending or posting messages or material that could damage the School's image or reputation.
- Creating a fake profile that impersonates any another member of the school community.
- Sending or posting material that is confidential to the School.
- Uses that violates copyright law, fail to observe licensing agreements or infringe on others intellectual property rights.
- Participating in the viewing or exchange of inappropriate images or obscene material.

While all cases involving the inappropriate use of social media will be dealt with on an individual basis, the school and its Board of Management considers the above to be serious breaches of our Code of Behaviour. Disciplinary consequences up to and including expulsion may be exercised in certain cases.

Please see the school's Code of Behaviour for information on the full range of sanctions the school employs and our appeal procedures.

3. Guidelines for staff on the use of Social Media sites.

Personal use of Social Media:

Use of these sites by staff in school is governed by Co. Offaly V.E.C. I.T Policy and the recently published 'Draft Code of Professional Conduct' from the Teaching Council. See Appendix C.

Staff should not use their personal profiles to conduct school business or communicate with Students or their Parents.

Educational use by staff:

Social Media sites can offer educational opportunities for collaboration on projects, presentation of ideas and sharing of class materials and resources. Staff should be guided by the following principles when incorporating Social Media into their teaching.

- The starting point for all Social Media interaction should be via a link in your Subject Department section on the school's website.
- The educational advantage of the use of the Social Media site in question should be clear and permission sought from the school Principal before use.
- Material that is confidential in nature such as student names, grades etc. should never be posted.
- 'Groups' should be used when collaborating on Facebook. Membership of these can be strictly controlled and users do not have to be friends of other users or the group's creator.
- Pay strict attention to intellectual property and copyright laws.
- All students participating in the online collaboration should be advised of their responsibility to use the site appropriately as per sections 1 & 2 above.
- Staff are expected to exercise sound judgement and maintain the highest professional standards while using Social Media in the school.

More information on how Facebook may be incorporated safely into the classroom and the creation of groups is contained in Appendix D.

ROLES AND RESPONSIBILITIES

1. The Board of Management will approve the policy and ensure its development and evaluation.
2. The Principal and Deputy Principal will be responsible for the dissemination of the policy and the application of consequences.

3. Year Heads will outline unacceptable uses of Social Media to students and be responsible for keeping records of breaches of Section 2 of the Policy.
4. The Principal, HSCL Teacher and the relevant Year Head will organise for the provision of a Parents Information Evening on Internet safety. This presentation should be organised in conjunction with Feeder Primary Schools and take place every two Years.
5. Class Tutors will be alert to the signs and possibilities of Bullying within their groups.
6. Strategies to ensure online safety will be taught as part of the SPHE anti-bullying programme.
7. Subject Teachers will report any incidents of online bullying and be mindful of their obligations under Child protection Guidelines.
8. The Guidance Counsellor and Care Team will provide support for students who have been victims on online bullying.
9. Programme Co-ordinators will ensure that their section of the school's website complies with this policy.
10. Subject Teachers will adhere to the guidelines outlined in Section 3 of the policy above.

REVIEW AND EVALUATION

The effectiveness of this policy will be monitored by the Principal and Deputy Principal.

The policy will be reviewed annually or as needs dictate during the academic year.

APPENDIX A

Follow the links below for resources to assist in educating students on the responsible use of the Internet and Social Media.

<http://www.makeitsecure.org/en/young-users.html>

<http://www.make-it-safe.net/>

<http://www.webwise.ie/>

<http://www.facebook.com/safety/groups/teens/>

<http://www.internetsafety.ie/website/ois/oisweb.nsf/page/safety-en>

www.watchyourspace.ie

www.thinkb4uclick.ie

www.safekids.com

APPENDIX B

Procedure for Alerting Facebook in the case of Bullying or the posting of inappropriate images.

The link below can be used to report the above to Facebook who generally take such reports seriously and quickly remove the offensive material.

<http://www.facebook.com/help/?page=178608028874393&ref=bc>

Procedure for Reporting a Fake Profile on Facebook.

The first piece of action to be taken by a person, in respect of whom a fake profile on Facebook has been set up, is to contact the Facebook Help Centre immediately and require Facebook to remove the fake profile. This can be done using the link to the Help Centre below. Facebook state that the profile will be removed within 24 hours from notification.

<http://www.facebook.com/help/?faq=167722253287296>

Procedure for having inappropriate or offensive clips removed from YouTube

YouTube may be alerted to inappropriate uses by selecting the 'Flag' option beside the clip. YouTube will then ask you to select one of six reasons why the video is inappropriate: Sexual Content; Violent or Repulsive Content; Hateful or Abusive Content; Harmful Dangerous Acts; Infringement of Personal Rights; Spam. Once you have indicated the reason YouTube will review the clip within 48 hours and delete it if necessary

APPENDIX C

Guidelines for staff on Personal use of Social Media websites

From the Teaching Council Code of Conduct

Teachers shall...

3.3.6 Communicate effectively with pupils/students, colleagues, parents, school management and others in a manner that is professional, collaborative and supportive, and based on trust and respect.

3.3.7 Ensure that any communication with pupils/students, colleagues, parents, school management and others is appropriate, including communication via electronic media, such as e-mail, texting and social networking sites.

3.3.8 Ensure that they do not access, download or otherwise have in their possession while engaged in school activities, inappropriate materials/images in electronic or other format.

3.3.9 Ensure that they do not access, download or otherwise have in their possession, at any time or in any place, illegal materials/images in electronic or other format.

County Offaly VEC I.T. Policy

Table of Contents

<u>Table of Contents</u>	9
<u>Introduction</u>	10
<u>1) Purpose of Use</u>	10
<u>2) Authorisation</u>	10
<u>3) Privacy</u>	11
<u>4) Behaviour</u>	11
<u>5) Definitions of Acceptable & Unacceptable Usage</u>	12
<u>6) Discipline</u>	13
<u>7) Policy Supervision and Advice</u>	13
<u>8) Legal Constraints</u>	13

Introduction

This Acceptable Use Policy is intended to provide a framework for such use of County Offaly VEC IT resources. It applies to all computing, telecommunication, and networking facilities provided by any section of County Offaly VEC.

1) Purpose of Use

County Offaly VEC resources are provided to facilitate a person's essential work as an employee of County Offaly VEC.

Any personal use of, and any work for outside bodies, using any piece of County Offaly VEC I.T. equipment is prohibited.

2) Authorisation

All individually allocated usernames, passwords and e-mail addresses are for the exclusive use of the individual, to whom they are allocated, as are individually allocated certificates, e.g. banking on line. The user is personally responsible and accountable for all activities carried out under their username. The password associated with a particular personal username must not be divulged to any other person, other than to designated members of IT staff for the purposes of system support. Attempts to access or use any username, e-mail address or certificate, which is not authorised to the user, is prohibited. No one may use, or attempt to use, IT resources allocated to another person, except when explicitly authorised by the provider of those resources.

All users must correctly identify themselves at all times. A user must not masquerade as another, withhold their identity or tamper with audit trails. A user must take all reasonable precautions to protect their resources. In particular, passwords used must adhere to current password policy and practice. This advice must be followed: failure to do so may be regarded as a breach of this policy.

Designated users have been given access to the system remotely to facilitate the access to email and data without the need to come to the office. While this practice is becoming more commonplace, the security risks associated with this cannot be overstated. As a result a new password policy has been put in place where each user must change their password every 30 days or sooner. The password must meet the complexity and history requirements of the policy before they will be accepted.

Email reports are configured to generate a daily report of backups. The designated IT support company will provide a quarterly test restore of data to a folder on the server and a full image restore to another suitable machine to validate the backup process. This is essential to ensure that Data Integrity is verified by checking backups in full.

Broadband usage within the VEC is through the Server firewall. To this end the Eircom Router has been locked down so that it will not provide internet through direct connection to the router itself. All inbound and outbound traffic is fully monitored and logged by username.

No unauthorised/unencrypted devices should be used to copy data to/from any laptop/PC/network drive. This is to ensure integrity of VEC data.

3) Privacy

It should be noted that the CEO/APO have the ability, which is occasionally required, to access all files, including electronic mail files, stored on the computer system which they manage. It is also occasionally necessary to intercept network traffic. In such circumstances the CEO/APO will take all reasonable steps to ensure the privacy of service users. County Offaly VEC fully reserves the right to monitor e-mail, telephone and any other electronically-mediated communications, whether stored or in transit.

Reasons for such monitoring may include the need to

- ensure operational effectiveness of services,
- prevent a breach of the law, this policy, or other County Offaly VEC policy,
- investigate a suspected breach of the law, this policy, or other Company policy,
- Monitor standards.
- County Offaly VEC sees staff privacy as desirable but not as an absolute right, hence staff should not expect to hold or pass information, which they would not wish to be seen by members of staff responsible for their work. In addition to when a breach of the law or of this policy is suspected, or when a documented and lawful request from a law enforcement agency such as the Gardaí or security services has been received, management are also authorised to release the contents of a staff files, including electronic mail files.

After a staff member leaves County Offaly VEC, files which are left behind on any computer system owned by County Offaly VEC, including servers, and including electronic mail files, will be considered to be the property of County Offaly VEC. When leaving County Offaly VEC staff should make arrangements to transfer to colleagues any e-mail or other computer-based information held under their personal account, as this will be closed on their departure.

The CEO and APO have access to daily, weekly and monthly reports on Internet and E-mail usage.

If there are websites that are currently blocked by Webmarshal software, and which need to be unblocked for work related reasons, a form must be completed and passed to the CEO for approval (see Appendix 1)

In line with confidentiality and security issues, changes are being made to the use of folders on shared network drives. Access to each person's individual folder on the network drive will be restricted to that person only. In recognition of the fact that cases may arise where a user needs access to information stored in another user's folder – access will be facilitated to specific folders within other user's main folders. Such access will only be permitted in exceptional circumstances. A form (see Appendix 2) is to be completed to allow this access.

4) Behaviour

No person shall jeopardise the integrity, performance or reliability of computer equipment, software, data and other stored information. The integrity of County Offaly VEC is put at risk if users do not take adequate precautions against malicious software, such as computer virus programs. All users of County Offaly VEC must ensure that any computer, for which they have responsibility, and which is attached to County Offaly VEC network, is adequately protected against viruses, through the use of up to date anti-virus software and has the latest tested security patches installed. Reasonable care should also be taken to ensure that resource use does not result in a denial of service to others.

Distributing material, which is offensive, obscene or abusive, may be illegal and may also contravene County Offaly VEC codes on harassment. Users of County Offaly VEC computer systems must make themselves familiar with, and comply with: [The Code of Practice for dealing with Complaints of Bullying and Harassment in VEC Workplaces](#) and [The Code of Practice for dealing with Complaints of Sexual Harassment in VEC Workplaces](#) .

No user shall interfere or attempt to interfere in any way with information belonging to or material prepared by another user. Similarly no user shall make unauthorised copies of information belonging to another user. The same conventions of privacy should apply to electronically held information as to that held on traditional media such as paper.

Users of services external to County Offaly VEC are expected to abide by any policies, rules and codes of conduct applying to such services. Any breach of such policies, rules and codes of conduct may be regarded as a breach of this Acceptable Use Policy and be dealt with accordingly.

5) Definitions of Acceptable & Unacceptable Usage

Unacceptable use of computers and network resources shall include

- the retention, propagation, accessing, sending, requesting, downloading transmitting or purposely viewing of material that is offensive, obscene, indecent, sexual, pornographic, racist, profane, violent or other offensive material via the Internet or E-Mail.
- Intellectual property rights infringement, including copyright, trademark and patent.
- causing annoyance, inconvenience or needless anxiety to others;
- unsolicited advertising, often referred to as "spamming";
- sending e-mails that purport to come from an individual other than the person actually sending
- attempts to break into or damage computer systems or data held thereon;
- actions or inactions which intentionally aid the distribution of computer viruses
- using the County Offaly VEC network for unauthenticated access;
- Use of the Internet & or E-mail in a manner which amounts to bullying or harassment

These restrictions should be taken to mean, for example, that the following activities will normally be considered to be a breach of this policy (potential exceptions should be discussed with senior management):

- the downloading, distribution, or storage of music, video, film, or other material, for which you do not hold a valid licence, or other valid permission from the copyright holder;
- the distribution or storage by any means of pirated software;
- connecting an unauthorised device to the County Offaly VEC network, i.e. one that has not been configured to comply with this policy and any other relevant regulations and guidelines relating to security, IT purchasing policy, and acceptable use;
- monitoring or interception of network traffic, without permission;
- probing for the security weaknesses of systems by methods such as port-scanning, without permission;
- associating any device to network Access Points, for which you are not authorised;
- non-work activities which generate heavy network traffic, especially those which interfere with others' legitimate use of IT services or which incur financial costs;
- the deliberate viewing and/or printing of pornographic images;
- the posting of defamatory comments about staff on social networking sites;
- the use of CDs, DVDs, and other storage devices for the purpose of copying the copying of other people's web site material without the express permission
- Plagiarism, i.e. the intentional use of other people's material without attribution.
- Anyone who uses a Registered Trade Mark without permission can expose themselves to litigation.
- Use of e-mail for personal use is prohibited
- You are prohibited from participating in social networking websites, such as by:
 - Registering with such sites
 - Accessing your own account on such sites
 - Accessing other peoples accounts on such sites or
 - Posting comments on other peoples sites.

It should be noted that individuals may be held responsible for the retention of attachment material that they have received, via e-mail that they have never opened, via e-mail that they have read. Similarly, opening an attachment, received via unsolicited e-mail, especially if clearly unrelated to work or study, which leads to widespread virus infection, may result in disciplinary action being taken.

6) Discipline

Staff members who break this Acceptable Use Policy will find themselves subject to disciplinary procedures and County Offaly VEC may take such disciplinary action. Individuals may also be subject to criminal proceedings. County Offaly VEC reserves its right to take legal action against individuals who cause it to be involved in legal proceedings as a result of their violation of licensing agreements and / or other contraventions of this policy.

7) Policy Supervision and Advice

Any suspected breach of this policy should be reported to the C.E.O. The C.E.O. will then take the appropriate action within County Offaly VEC disciplinary framework. IT Services staff will also take action when infringements are detected in the course of their normal duties. Actions will include, where relevant, immediate removal from online information systems of material that is believed to infringe the law. County Offaly VEC reserves the right to audit and / or suspend without notice any account pending any enquiry. Where necessary, this will include the interception of electronically mediated communications.

This policy is not exhaustive and inevitably new social and technical developments will lead to further uses, which are not fully covered. In the first instance staff should address questions concerning what is acceptable to their supervisor; where there is any doubt the matter should be raised with the C E O, who will ensure that all such questions are dealt with at the appropriate level within County Offaly VEC.

8) Legal Constraints

Introduction

Any software and / or hard copy of data or information which is not generated by the user personally and which may become available through the use of County Offaly VEC computing or communications resources shall not be copied or used without permission of County Offaly VEC or the copyright owner. In particular, it is up to the user to check the terms and conditions of any licence for the use of the software or information and to abide by them. Software and / or information provided by County Offaly VEC may only be used as part of the user's duties as an employee of County Offaly VEC.

NB** The user must abide by all the licensing agreements for software entered into by County Offaly VEC with other parties, noting that the right to use any such software outside County Offaly VEC will cease when an individual leaves the VEC. Any software on a privately owned computer that has been licensed under County Offaly VEC agreement must then be removed from it, as well as any County Offaly VEC data.

All software licensing is the responsibility of the management who authorise the installation. A form will need to be completed for any PC / laptop that require VEC licensed software (see Appendix 3). Such requests for licensing will need to be authorised by the CEO. Terms and conditions of Software licensing agreements are available on request.

You are prohibited from using the Internet outside of the workplace where such use has the potential to negatively affect County Offaly VEC or its staff. Examples of such behaviour include:

- Publishing material which is defamatory, abusive or offensive in relation to any employee, manager, office holder, customer or client of County Offaly VEC
- Using the Internet in a manner which amounts to bullying or harassment
- Publishing any organisation-sensitive information about County Offaly VEC
- Publishing material which might reasonably be expected to have the effect of damaging the reputation or professional standing of County Offaly VEC or its staff

In the case of private work and other personal use of computing facilities, County Offaly VEC will not accept any liability for loss, damage, injury or expense that may result.

The user must comply with all relevant legislation and legal precedent, including the provisions of the Data Protection Act.

APPENDIX D

The link below will take you to Facebook's gateway page for information on using Facebook in the classroom

<http://www.facebookforeducators.com>

This table provides a list of Facebook sites that may be of use in the classroom.

Facebook Pages for Educators	
National Geographic Education	http://www.facebook.com/natgeoeducation
British Museum	http://www.facebook.com/britishmuseum
Girl Up (UN Foundation)	http://www.facebook.com/girlup
NASA	http://www.facebook.com/NASA
Smithsonian Institution	http://www.facebook.com/SmithsonianInstitution
Youth Olympic Games	http://www.facebook.com/youtholympicgames
Library of Congress	http://www.facebook.com/libraryofcongress
Musee du Louvre	http://www.facebook.com/museedulouvre
PBS Kids	http://www.facebook.com/PBSKIDS
Kabul Museum	http://www.facebook.com/pages/Kabul-Museum/317714056516
Discovery Channel Global Education	http://www.facebook.com/DCGEP
Scholastic Teachers	http://www.facebook.com/ScholasticTeachers
Facebook in Education	http://www.facebook.com/education
Get Schooled Foundation	http://www.facebook.com/GetSchooledFoundation
Encyclopaedia Britannica	http://www.facebook.com/BRITANNICA
Facebook for Educators	http://www.facebook.com/fb4educators

This link provides information on how to use Facebook groups and further information on integration of Facebook into lessons.

<http://facebookforeducators.org/>