

Our Lady of Mercy College

Beaumont,

Dublin 9

Internet & Website Acceptable Usage Policy(AUP)

Internet & Website Acceptable Usage Policy(AUP)

1. Mission Statement

Our mission statement states that the core value of Our Lady of Mercy College Beaumont is respect for all and the nurturing of individual potential, academically, spiritually and culturally as a member of the school community and in the spirit of the Mercy Ethos.

2. Scope

This policy addresses the rights, privileges, responsibilities and sanctions associated with the use of computers and the internet in Our Lady of Mercy College. It has been drawn up by school staff, students, parents and Board of Management. It identifies the school strategies for the safe use of the internet. This policy address all aspects of Internet usage at school, e.g browsing the internet, using search engines, downloading, publishing a school website, using email and chatrooms etc.

3. Rationale

The aim of this Internet & Website Acceptable Usage Policy is to ensure that pupils will benefit from learning opportunities offered by the school's Internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. Therefore, if the school AUP is not adhered to this privilege will be withdrawn and appropriate sanctions – as outlined in the AUP – will be imposed. It also ensures that staff use of computers is in line with best practice in the workplace.

4. School's Strategy

The school employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

4.1 General

- Internet sessions will always be supervised by a teacher.
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material.
- The school will regularly monitor pupils' Internet usage.
- Students and teachers will be provided with training in the area of Internet safety.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- The use of personal ~~floppy disks~~, memory sticks, CD-ROMs, or other digital storage media in school requires a teacher's permission. Students are encouraged to use cloud computing.
- Students will treat others with respect at all times and will not undertake any actions that may bring the school into disrepute.
- Information and Computer Technology (ICT) equipment & software remain the property of the school.

4.2 World Wide Web

- Students will not intentionally visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.

- Students will report accidental accessing of inappropriate materials in accordance with school procedures.
- Students will use the Internet for educational purposes only.
- Students will not copy information into assignments nor will they fail to acknowledge the source (plagiarism and copyright infringement).
- Students will never disclose or publicise personal information.
- Downloading by students of materials or images not relevant to their studies is in direct breach of the school's acceptable user policy.
- Downloading, uploading & streaming of data which pertains to school activities/staff/ or other students without the permission of staff is in ~~and not relevant to the students' studies, is in~~ direct breach of the school's acceptable use policy. Users shall not make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments relating to school activities without permission.
- Students will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

4.3 Email

- Students will use approved class-school email accounts under supervision by and with the permission of their teacher.
- Students will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person.
- Students will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.
- Students will never arrange a face-to-face meeting with someone they only know through emails or the internet.
- Students will note that sending and receiving email attachments is subject to permission from their teacher.

4.4 — Internet Chat 4.4 Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following tables shows how the school currently considers the benefit and risks/disadvantages of using these technologies for education:

<u>Communication Technologies</u>	<u>Allowed</u>	<u>Allowed with staff permission</u>	<u>Not allowed</u>
<u>Mobile phones may be brought to school.</u>	√		
<u>Use of mobile phone in lessons</u>		√	
<u>Use of mobile phone in social time. Morning break and lunchtime</u>	√		
<u>Taking photos on mobile phones or with other devices</u>			√
<u>Use of handheld devices eg PDAs, PSPs etc..</u>			√

<u>Use of school email for personal emails</u>			<u>√</u>
<u>Use of chat rooms/facilities</u>			<u>√</u>
<u>Use of instant messaging</u>			<u>√</u>
<u>Use of social networking sites</u>			<u>√</u>
<u>Use of blogs</u>		<u>√</u>	

Inappropriate Activities:

<u>Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:</u>	<u>Child sexual abuse images</u>	<u>Unacceptable & illegal</u>
	<u>promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation</u>	
	<u>racist material</u>	
	<u>pornography</u>	
	<u>promotion of any kind of discrimination promotion of racial or religious hatred</u>	<u>Unacceptable</u>
	<u>threatening behaviour, including promotion of physical violence or mental harm</u>	
	<u>any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute</u>	
<u>Using school systems to run a private business</u>		<u>Unacceptable</u>
<u>Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed the school</u>		<u>Unacceptable</u>
<u>Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions</u>		<u>Unacceptable</u>
<u>Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer / network access codes and passwords)</u>		<u>Unacceptable</u>
<u>Creating or propagating computer viruses or other harmful files</u>		<u>Unacceptable</u>
<u>Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet</u>		<u>Unacceptable</u>
<u>On-line gaming</u>		<u>Unacceptable</u>
<u>On-line gambling</u>		<u>Unacceptable</u>
<u>On-line personal shopping/commerce</u>		<u>Unacceptable</u>
<u>File sharing</u>		<u>Unacceptable</u>
<u>Use of social networking sites</u>		<u>Unacceptable</u>

4.4

4.5 ~~Students will only have access to chat rooms, discussion forums, messaging or other electronic communication fora that have been approved by the school.~~

4.6 ~~Chat rooms, discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.~~

4.7 ~~Usernames will be used to avoid disclosure of identity.~~

4.8 ~~For reasons of personal safety students should not have face-to-face meetings with someone organised via Internet chat rooms.~~

4.5 School Website

- Pupils will be given the opportunity to publish projects, artwork or school work on the Internet 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 will be checked frequently 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 the parental permission. ~~Video clips may be password protected.~~
- Personal pupil information including home address and contact details will be omitted from school web pages.
- The school website will avoid publishing the first name and last name of individuals in a photograph.
- 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.

5. 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/~~other device-camera~~, still or moving is in direct breach of the school's Acceptable Use Policy and Mobile Phone/Electronic Equipment Policy.

6. Legislation

The school will provide information on the following legislation relating to use of the Internet which teachers, students and parents should familiarise themselves with: (see Appendix 2)

- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video Recordings Act 1989
- The Data Protection Act 1988

7. Support Structures

The school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet.

8. Sanctions

Misuse of the Internet will 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.

9. Staff Use of Computers:

ICT is recognised as being an excellent support to teaching & learning as well as to other school activities. Our Lady of Mercy College, Beaumont encourages the use of ICT by its staff and it provides computers for staff use for school related activities. Computers are available in the classrooms and extra computers are provided in the staff workrooms and may be used during non timetabled classes.

The use of personal laptops and other equipment devices to access the schools wifi is permitted. networks is prohibited unless authorised by the Principal. Staff are expected to keep their anti-virus up to date. Storage devices such as memory sticks should be used prudently, i.e. scanned with anti virus software before using if used in the school.

Teachers may as part of their teaching use ICT to record students or they may ask students to submit digital recordings. This is done for teaching and assesment purposes only thus enhancing the students learning experience.

Staff adhered to best practice in the use of Virtual Learning Environments (VLE's) in the school setting. E-portal is also used for administration purposes and neither one is used in a public setting.

Best practice to do with internet use is paramount to the school and filters are in place to safeguard all those in the school community. These must be respected and all users of ICT have a responsibility to ensure that the school network is only used to download, upload, store, distribute or otherwise use work related material. Under no circumstances should non work related music or video or unlicensed software be accessed.

Staff members are expected to use these resources in a professional, responsible, ethical and lawful manner.

No student or staff member may offer an opinion via blogs, chatrooms etc. on behalf of the school.

10. Use of Imaging Equipment and Digital Media

Digital imaging equipment covers any piece of equipment which can be used to create an electronic image. This includes such devices as CD Rewriters, digital cameras, camera phones, photocopiers, scanners, tablets but is not limited to these devices exclusively.

Staff who use digital imaging equipment in the course of their duties must ensure that they do so in a legal and appropriate manner.

11. Compliance with Applicable Laws and Licenses

Staff & Students must comply with software licenses, copyrights and all other local, national and international laws governing intellectual property and online activity.

12. Related Policies:

Anti Bullying Policy

Code of Behaviour

Use of Mobile Phone & Electronic Equipment Policy

Pastoral Care Policy

Guidance & Counselling Policy

Expulsion Policy

SPHE Policy

Vetting Policy

13. Training:

Staff members will be provided with training in the area of internet safety. Students will be reminded of the content of the policy through their classes.

14. Implementation & Monitoring

Parents are expected to read the AUP carefully before signing up to it on enrolling their daughter in the college(see appendix 1). All staff members have a role in ensuring that it is implemented and together with the ICT committee will ensure that standards set down here in will be achieved.

15. Review:

This policy will be review every three years in line with Board of Management Policy. If a need arises it can be reviewed before this.

Ratified December 11th 2014

Signed:
(for and on behalf of the Board of Management)

Appendix 1

Advice to Parents/Guardians

Re: Internet & Website Acceptable Usage Policy

As part of the school's education programme we offer pupils supervised access to the Internet. This allows students access to a large array of online educational resources that we believe can greatly enhance students' learning experience.

However, access to and use of the Internet requires responsibility on the part of the user and the school. These responsibilities are outlined in the school's Acceptable Use Policy. It is important that this policy is read carefully, signed by a parent or guardian and returned to the school.

Although the school takes active steps to promote safe use of the Internet, it recognises the possibility that students may accidentally or deliberately access inappropriate or objectionable material.

The school respects each family's right to decide whether or not to allow their children access to the Internet as defined by the school's Acceptable Use Policy.

Having read the terms of our school's Acceptable Use Policy, you may like to take a moment to consider how the Internet is used in your own home, and see if there is any way you could make it safer for your own family.

Please discuss this policy with your daughter. You are asked to tick acceptance of this policy by completing the relevant section on the Entry/Renewal Form (submitted on enrolling each year).

Before completing your response on the Entry/Renewal form please consider the following.

As the parent or legal guardian of the above pupil, I have read the Internet and Website Acceptable Use Policy and grant permission for my daughter or the child in my care to access the Internet. I understand that Internet access is intended for educational purposes. I also understand that every reasonable precaution has been taken by the school to provide for online safety but the school cannot be held responsible if pupils access unsuitable websites.

In relation to the school website, I accept that, if the school considers it appropriate, my child's schoolwork may be chosen for inclusion on the website. I understand and accept the terms of the Acceptable Use Policy relating to publishing children's work on the school website.

Appendix 2

Internet Safety, Pieces of Legislation

There is no specific legislation governing Internet safety at school level. The internet functions in a global context whereas the law operates in a localised one. There are, however, a number of legislations that have relevance to Internet safety. They are briefly described as follows:

Data Protection Act 1988

This act was passed in order to deal with privacy issues arising from the increasing amount of information kept on computer about individuals.

Data Protection (Amendment) Act 2003

This amendment extends the data protection rules to manually held records and also makes improvements to the public's right to access data.

Child Trafficking and Pornography Act 1998

This act legislates against anyone who knowingly produces, prints, publishes, distributes, exports, imports, shows, possesses or sells child pornography.

Interception Act 1993

(The Interception of Postal Packets and Telecommunications Messages Regulation Act 1993). This act stipulates that telecommunication messages can be intercepted for the purpose of an investigation of a serious offence. Authorisations are subject to certain conditions.

Video Recordings Act 1989

This act prohibits the distribution of videos which contain obscene or indecent material which may lead to the depravation or corruption of the viewer. It would apply where someone in the State supplied this kind of video over the Internet.

Appendix 3

Form given to Computer Co-ordinator at the beginning of the School Year

Completed by the Class Tutor, first week in September.

Internet & Website Acceptable Usage Policy (AUP)

To be completed by the Class Tutor at the end of the first week of term indicating those who have accepted/not accepted the schools policy as asked on the Entry/Renewal Form.

Record those who do not accept the schools policy regarding online access & safety and the schools policy regarding the publishing of work on the schools website

School Year			
Class			
Tutor			
Those who do not accept the schools policy regarding the publishing of work on the schools website			