

ABBAY VOCATIONAL SCHOOL DONEGAL TOWN



Internet – Acceptable Use Policy

Adopted by BOM June 2011

Amended May 2017

Slight amendment November 2018

Amended April 2020 (Covid 19)

The aim of this *Acceptable Use Policy (AUP)* 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 Therefore, if the school *AUP* is not adhered to this privilege will be withdrawn and appropriate sanctions – as outlined in the *AUP* – will be imposed.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 is envisaged that school and parent representatives will revise the *AUP* annually. Before signing, the *AUP* should be read carefully to ensure that the conditions of use are accepted and understood.

A second version of the *AUP* was revised in June 2011 by *all the parties involved in the Abbey Vocational School*.

A further version of the *AUP* was revised in Feb 2017 by *all the parties involved in the Abbey Vocational School and further amended in November 2018*.

It has been updated in light of Covid 19 in April 2020 to include a section on teleconferencing

School Strategy

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

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.
- 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.
- Access to personal storage must be supervised by a teacher.

- Students will observe good “netiquette” (i.e. etiquette on the Internet) at all times and will not undertake any actions that may bring the school into disrepute.

World Wide Web

- Students will not visit Internet sites that contain obscene, illegal, or otherwise objectionable materials.
- Students will use the Internet for educational purposes only.
- Students will be familiar with copyright issues relating to on-line learning.
- Students will never disclose or publicise personal information.
- 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.

Email

- Students will use approved class email accounts under supervision by or permission from a 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.

Internet Chat

- Students will only have access to chat rooms, discussion forums or other electronic communication forums 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 which has been approved on the World Wide Web under the supervision of a teacher.
- 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.
- Digital photographs, audio or video clips of individual students will not be published on the school website. Instead photographs, audio and video clips will focus on group activities. Video clips may be password-protected.
- Personal pupil information including home address and contact details will be omitted from school web pages.
- Pupils will continue to own the copyright on any work published.

Teleconferencing

Our school utilises teleconferencing during periods of school closure. Distance learning is a way of learning remotely without being in regular face-to-face contact with a teacher in the classroom. There are many benefits to teaching and learning in this way, and students and teachers have the tools and expertise to use teleconferencing to sustain learning.

Our school provides a teleconferencing option for our students and staff. It is expected that students and staff will use the platform in a professional and ethical manner for the purpose of teaching, learning and Assessment.

The use of teleconferencing requires students and teachers to observe the following rules in order to ensure that both staff and students benefit from this way of teaching and learning. Students and Staff should never;

- Post, stream or transmit any content, including live video, that violates this Policy in such a way that is offensive to students / staff.
- Do anything illegal, facilitate any illegal activity, or promote violence.
- Do anything that threatens, exploits or otherwise harms children or fellow students.
- Engage in any activity that is harmful, obscene, or indecent. This includes offensive gestures, displays of nudity, violence, pornography, sexually explicit material, or criminal activity.
- Engage in any activity that is fraudulent, false, or misleading.

- Engage in any activity that is defamatory, harassing, threatening or abusive.
- Store or transmit any data or material that is fraudulent, unlawful, harassing, libelous, threatening, obscene, indecent or otherwise inappropriate.
- Send unauthorized messages or irrelevant material.
- Misrepresent a user's identity or affiliation with any entity or organization, or impersonate any other person.
- Harvest, collect, or gather user data without consent.
- Violate or infringe any intellectual property or proprietary rights of others, including copyrights.
- Violate the privacy of others or distribute confidential or personal information of others.
- Engage in any activity that is harmful or disruptive to the operation of on-line classes. This includes transmitting viruses, malware or other malicious or destructive code or using tools that mask IP address location or to otherwise circumventing restrictions on use due to regulations or account closures.

If school authorities are made aware of any abuse or infringement on these rules, the school will investigate the issue and take immediate, appropriate action where warranted in line with the school's Code of Behaviour.

Personal Devices:

Students using their own technology in school should follow rules set out in this agreement. They will only use hand held /external devices (mobile phones /USB devices) in school if they have permission and **under strict teacher supervision**. Please also see mobile phone policy.

1. Any pupil/student whose teacher wishes them to use a personally owned mobile device within school must read and sign the Acceptable Use Policy (AUP) section and the Mobile Phone Policy section in the school journal (page 3).

2. A parent /guardian of the pupil/student must also read, sign the Acceptable Use Policy (AUP) section and the Mobile Phone Policy section in the school journal (page 3).

3. Students take responsibility for appropriate use of their device at all times. The school is not responsible in any way for the device or for its use.
4. Students/parents/guardians are responsible for their devices, including any breakages, costs of repair, or replacement.
5. The Principal and Deputy Principals reserve the right to inspect or monitor student mobile devices during school hours.
6. Violations of any school policies or rules involving a student device may result in a student not being allowed continue using the device during school hours and/or disciplinary action, for a period to be determined by the school.
7. During school hours students are allowed use their device for learning related activities **only and only at the instruction of the teacher.**
8. Students will comply with teachers' requests regarding use of devices during school hours, and classes. Special accommodations will apply to school tour abroad as outlined in the excursion policy
9. Mobile devices must be charged prior to bringing them to school so as to be usable during school hours. Charging devices in the school is not permitted.
10. Students may not use the devices to record, transmit or post photos or video of other teachers or students. No images or video recorded at school can be transmitted or posted at any time without the permission of their teachers.
11. Student may use the school wireless network and content filtered broadband. Use of other 'unfiltered public wireless connections, such as mobile networks, is not allowed during school hours.

In order to ensure that photos and videos are being used safely:

- Any pictures should try to focus on group activities, rather than photos of an individual. Group photos should always be preferred over full face pictures of individual children.

- Names, especially full names, should not be used, and if they are, the names need to be kept separate from images.
- Students will be educated about the risks associated with the taking, using, sharing, publication and distribution of images. In particular, teachers will recognise the risks attached to publishing their own images on the internet
- When taking digital/video images ensure that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Students must not take, use, share, or publish images of others without consent
- Pictures to be published on the school's website, or elsewhere, which include pupils will be selected carefully and will comply with good practice guidance on image use
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of students are published on the school website
- Student work can only be published with the permission of the student and parents or carers.

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:

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

The above list of legislation is not exhausted, and teachers, students and parents should familiarize themselves with all the relevant legislation. Breach of all of the above legislation will be considered to be a breach of discipline

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.

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.

Cyber Bullying

Please read the cyber bullying policy at the bottom of this policy for an outline of expectations in this regard.

Permission Form Template

Please review the attached school Internet Acceptable Use Policy. This should be signed in the student’s school journal at the commencement of every school academic year.

Name of Student: _____

Class/Year: _____

Student: I agree to follow the school’s Acceptable Use Policy on the use of the Internet. I will use the Internet in a responsible way and obey all the rules explained to me by the school. I accept that it is my responsibility to be familiar with all relevant legislation to the use of internet and mobile devices.

Student’s Signature: _____ **Date:**

Parent/ Guardian Signature: _____ **Date:**

ABBHEY VOCATIONAL SCHOOL

DONEGAL TOWN



Anti Cyber Bullying Policy

Amended April 2020 Covid 19

Abbey Vocational School Anti-Cyberbullying Policy

Introduction

Cyberbullying can be very damaging to individuals, and disruptive to school life. Though new technology brings incredible opportunities for educators as well as young people, it is crucial that everyone knows how to use this technology responsibly and that policies are in place to support and encourage responsible use.

Scope

This document is aimed at combating cyberbullying. Cyberbullying includes (but is not limited to) communicating via electronic means with the objective of causing hurt, fear, embarrassment, humiliation, alarm and/or distress to one or more persons. Cyberbullying includes the use of mobile phones and the internet with the objective of upsetting someone. It

may take the form of general insults or impersonation, defamation or prejudice-based bullying.

While this policy addresses issues related to the cyberbullying of students (i.e. situations in which one or more students are the victim(s) of bullying), the policy also applies to teaching and other school staff, parents/guardians, and others insofar as measures under the policy relate to them.

This policy applies to activities and events that take place:

- During school time (including break times)
- Going to and from school
- On school tours/trips
- During extra-curricular activities
- During school closures where online learning is taking place
- Furthermore, [The Abbey Vocational School] reserves the right to take action against bullying perpetrated outside the school which spills over into the school. [SEP]

Objectives

This policy aims to ensure that:

1. Students, staff and parents know about cyberbullying and its effects;
2. Members of the school community have the knowledge, policies and procedures to prevent and, if necessary, to deal with cyberbullying in school or within the school community; and
3. The school monitors the effectiveness of its procedures and amends them where necessary.

The Abbey Vocational School is committed, to the extent permissible by available resources, to helping members of the school community to enhance their learning experiences through the use of modern technology. The school acknowledges that Information and Communication Technologies can play an important role in supporting learning, but also that they can be misused and can present risks.

The School aims to equip members of the school community with the skills and knowledge needed to use these technologies in a safe and responsible manner and to assisting those that encounter difficulties. The School also recognises that it must be vigilant towards bullying perpetrated outside School which spills over into the School.

The Abbey Vocational School aims to create a caring environment where those in the school community can work and learn without fear of being bullied. [Insert Name of School] aims to educate and inform its students as to how to use communications technology responsibly and

about the serious consequences of cyberbullying and will continue to inform and educate its students in these fast changing areas.

Goals

- To create a school ethos which encourages students to disclose and discuss incidents of cyberbullying behaviour.
- To raise awareness of cyberbullying as an unacceptable form of behaviour with school management, teachers, students, parents/guardians.
- To ensure that the school's Social, Personal and Health Education programme raises awareness of the factors associated with cyberbullying behaviour and develops students' appropriate knowledge, skills and behaviours.
- To take practical actions to prevent incidents of cyberbullying behaviour e.g. to ensure comprehensive supervision and monitoring measures through which all areas of school activity are kept under observation.
- To develop procedures for reporting and recording incidents of cyberbullying behaviour.
- To develop procedures for investigating and dealing with incidents of cyberbullying behaviour.
- To develop a programme of support for those affected by cyber-bullying behaviour and those involved in cyberbullying behaviour.
- To work with, and through, the various local agencies in countering all forms of cyber-bullying and anti-social behaviour.

Key Measures

The Principal will act, or will appoint a staff member to act, as a Cybersafety Officer, to oversee the practices and procedures outlined in this policy and monitor their effectiveness.

The Cybersafety Officer will ensure that the school maintains details of agencies and resources that may assist in preventing and addressing bullying.

Staff will be trained to identify signs of cyberbullying and will be helped to keep informed about the technologies that children commonly use.

A code of advice will be developed, periodically reviewed and communicated to help students protect themselves from being involved in bullying (as perpetrator or as victim) and to advise them on reporting any incidents.

Students will be informed about cyberbullying in the course of their education at the School.

Students and staff are expected to comply with the school's policy on the use of computers in the School.

Parents will be provided with information and advice on cyberbullying.

Definition of Cyber-Bullying:

Cyberbullying is aggression conducted by an individual or a group against others - such aggressive behaviour being committed via electronic means or via exclusion from electronic communities or interactions. Cyberbullying includes (but is not limited to) the communicating via electronic means with the objective of causing hurt, fear, embarrassment, humiliation, alarm and/or distress to one or more persons. Cyberbullying includes is the use of mobile phones and the internet with the objective of upsetting someone. It may take the form of general insults or impersonation, defamation or prejudice-based bullying. ^[L]_[SEP]

Types of behaviour involved:

These guidelines provide assistance in identifying and describing the types of behaviour involved in cyber-bullying. The means of cyber-bullying are constantly changing and the following list of types of bullying behaviour can be expanded in light of the experience of the school community:

Hate sites

Building websites that are dedicated to making fun out of someone.

Encouraging other people to join the bullying by publishing someone's personal details or linking to their social network page.

Abusive messages

Transmitting abusive and/or threatening messages.

Chat rooms and discussion forums

- Posting cruel and/or or abusive comments about someone.

Mobile phone

Sending humiliating and abusive video, photographic or text images/messages.

Making silent or abusive phone calls.

Sending abusive text messages.

Interactive gaming

Locking victims out of games.

Spreading false rumours about someone.

Hacking into someone's account.

Sending viruses

Sending hacking programs to another person.

Unauthorised interference with a computer device.

Abusing personal information

Transmitting personal photos, videos or emails.

Blogs

Posting blogs where others could see them without the owner of the blog's permission.

Prevention and Response

The school informs students about cyber bullying and also takes available steps to counter and respond to it.

The following measures represent the core of the School's anti cyber-bullying activities:

- A positive school culture and climate;
- School-wide approach;
- Effective leadership;
- A shared understanding of what bullying is and its impact;
- Anti-bullying policies;
- Consistent recording of reported bullying behaviour;
- Education and training;
- Prevention strategies including awareness raising;
- Intervention strategies.

The Abbey Vocational School trains its staff to respond effectively to reports of cyber-bullying or harassment and has systems in place to respond to it.

The Abbey Vocational School schools record all reported incidents of bullying behaviour including anonymous bullying reports.

The Abbey Vocational School provides information on cyber-bullying to all members of the school community. [SEP]

The Abbey Vocational School engages prevention and awareness raising measures and implements strategies to engage students in addressing problems when they see them.

The Abbey Vocational School is a “telling school”. If a member of the school community “speaks out” and reports an incident of cyber-bullying appropriate action will be taken.

The Abbey Vocational School endeavours to block access to inappropriate web sites, using firewalls, antivirus protection and filtering systems and no pupil is allowed to work on [SEP]the Internet in the Computer Room, or any other location within the school which may from time to time be used for such work, without a member of staff present whilst education and guidance remain at the center of what we do.

The Abbey Vocational School reserves the right to take disciplinary action (up to and including suspension and expulsion) against those who take part in cyber-bullying.

The Abbey Vocational School supports victims and, when necessary, will work with the Gardaí and other State agencies to identify those involved in criminal acts and to support victims.

The Abbey Vocational School will use, as appropriate, the full range of sanctions to correct, punish or remove pupils who bully fellow pupils or harass staff in this way, both inside and outside the school.

All members of the School community are aware they have a duty to bring to the attention of the Principal any example of cyberbullying or harassment that they know about or suspect.

The Abbey Vocational School Cyberbullying Critical Incident Form/Checklist

1. Reporting Details

Name of Person reporting the incident
Name of Staff member recording incident
Anonymous Report?
Date of report

2. Type of bullying incident (please tick all that apply; this list is not exhaustive)

Via mobile or hand-held device	
Face to Face	Involves Internet
Involves chatrooms	Involves IM
Blackberry Messenger	Involves SNS
Ridicule/humiliation	Friendship feud
Persistent teasing/sarcastic remarks	Demanding money/valuables
Name calling	Involves photographs or videos
Threats	Coercion
Spreading rumours	Encouraging others to join in
Unpleasant/hurtful email/texts/web posts combined	Provocative/sexist taunts
Plans to isolate someone	Linked to bullying in school
Other	Involves Internet

Racist*	Cyberbullying
Homophobic	Due to disability
Sexual	
*If racist report to local authority/The Gardaí /BOM or VEC – as appropriate	

3. Persons involved in incident

Name of victim/target	
Class	Year
Age	

Name of Perpetrator (s)	
1.	

2.	
3.	_____
Class	Year
Age (s)	..

4. Incident Details

Date(s) of incident
Day
Month
Year
Approximate times
Before school
Morning
Afternoon
After school
Weekend
Is this a one off incident/event?
How long has this been going on?
Has any intervention been tried?
If Cyberbullying, has this abuse been reported to the service provider or website administrator?
Is there evidence available e.g. screenshots, printouts?
Do the Gardaí need to be informed?
Does a device need to be confiscated or a computer isolated as evidence?
Does material need to be taken down from social media website?
Have parents of both students been alerted?
Who has taken responsibility for the above steps?

If you are not sure what steps to take, talk to your e-safety lead persons in school i.e. the Principal.

5. Follow up

Has the bullying stopped?
Does the target/victim feel safe?
Is further action required?
Have those involved changed their behaviours/acknowledged the harm caused?
Has the case contributed to the learning of the class/year/group in some way?
Have passwords been changed, privacy settings checked, and friends list cleaned?

Any further note such as the impact of this incident or recommendations:

Signed:

Date:

Position:

Letter to Parents/ Guardians:

Dear Parent/Guardian,

As part of the school's education programme we offer pupils supervised access to the Internet. This allows student's 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 (enclosed). It is important that this enclosed document 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.

Yours faithfully,

Geraldine Diver .
Principal.

