Ashbourne Community School
Acceptable Use Policy

This policy covers use of digital technologies in school, that is, email, internet, intranet and network resources, learning platform, software, equipment and systems and has been drawn up to protect everyone. The provisions of this policy also apply to access to the internet and email via remote devices such as smart phones and laptops.

1. PURPOSE

Ashbourne Community School owns and operates a variety of computing systems, which are provided for the use of Ashbourne Community School students/learners (including Adult Education programme) and staff in support of the programs of the school and are to be used for education, research, academic development, and public service only. All **users*** of these systems are responsible for seeing that these computing facilities are used in an effective, efficient, ethical, and lawful manner. This document establishes rules and prohibitions that define acceptable use of these systems. Unacceptable use is prohibited, and is grounds for loss of computing privileges, as well as discipline or legal sanctions.

***User definition:** A user is defined as an individual who uses a digital device.

This document establishes the need for an ICT Development Officer and an ICT Coordinating Committee.

The task of the ICT development officer/committee is to:

1. Set hardware and software purchasing plans, secure an annual budget and provide an annual budget breakdown
2. Ensure that there is an ongoing program of staff development and support.
3. Regularly review hardware, software and ICT training needs.
4. Co-ordinate where necessary with resource leaders in other curriculum areas, particularly in respect to software purchases.

The position of ICT Development Officer may be established and filled in line with the scheme of school needs. If not, the position of ICT Development Officer will be filled by agreement amongst the ICT Coordinating committee at the beginning of the academic year. Preferably all members of said committee will be involved in ICT at any level in the academic year. The Principal or other staff member designated by him / her will be a member of the committee. The ICT technician will have the option of attending meetings if he should so wish.

2. AUDIENCE AND AGREEMENT

All users of Ashbourne Community School computing systems must read, understand, and comply with the policies outlined in this document, as well as any additional guidelines established by the Information Technology Department. Such guidelines will be reviewed by the ICT Development Officer and may become subject to Board approval as a policy or procedure to be included in the school plan.

3. RIGHTS

BY USING ANY OF THESE SYSTEMS, USERS AGREE THAT THEY WILL COMPLY WITH THESE POLICIES.
These computer systems, facilities, and accounts are owned and operated by Ashbourne Community School. Ashbourne Community School reserves all rights, including termination of service without notice, to the computing resources that it owns and operates. These procedures shall not be construed as a waiver of any rights of the school, nor shall they conflict with applicable acts of law.

4. PRIVILEGES

Access and privileges on Ashbourne Community School computing systems are assigned and managed by the ICT Development Officer. Eligible individuals may become authorized users of a system and be granted appropriate access and privileges by following the approval steps prescribed for that system by the ICT coordinating committee. The ICT Development Officer must approve all access to the School's computer resources, including the issuing of accounts and related passwords.
Users may not, under any circumstances, transfer or confer these privileges to other individuals. Others shall not use any account assigned to an individual without express permission from the ICT Development Officer. The authorized user is responsible for the proper use of the system, including any password protection.

5. RESPONSIBILITIES

Users are responsible for maintaining the following:

a) **An environment in which access to all School computing resources are shared equitably between users.** The ICT Development Officer along with the ICT coordinating committee sets minimum guidelines within which users must conduct their activities.

b) An environment conducive to learning:

- A user who brings food or drink into the computer rooms will be asked to leave and privileges may be removed.
- Disruptive behaviour will not be tolerated in any form. If any arises, the user responsible will be denied access to the system and will be given alternative written work to complete at that time.
- A user who harasses, or makes defamatory remarks, shall bear full responsibility for his or her actions. Further, by using these systems, users agree that individuals who transmit such remarks, to or from the school, shall bear sole responsibility for their actions.
- Users agree that Ashbourne Community School's role in managing these systems is only as an information carrier, and that they will never consider transmission through these systems as an endorsement of said transmission by Ashbourne Community School. Some of the Ashbourne Community School computing systems provide access to outside networks, both public and private, which furnish electronic mail, information services, bulletin boards, conferences, etc. Users are advised that they may encounter material that may be considered offensive or objectionable in nature or content. Users are further advised that Ashbourne Community School does not assume responsibility for the contents of any of these outside networks. The user agrees to comply with the acceptable use guidelines for whichever outside networks or services they may access through Ashbourne Community School systems. Further, the user agrees to follow proper etiquette on outside networks. Documents regarding etiquette are available through the ICT Development Officer.
- The user agrees never to attempt to transmit, or cause to be transmitted, any message in which the origination is deliberately misleading (except for those outside services which may conceal identities as part of the service). The user agrees that, in the unlikely event that someone does transmit, or

cause to be transmitted, a message that is inconsistent with an environment conducive to learning or with a misleading origination, the person who performed the transmission will be solely accountable for the message, not Ashbourne Community School, which is acting solely as the information carrier.

c) **An environment free of illegal or malicious acts:** The user agrees never to use a system to perform an illegal or malicious act. Any attempt to increase the level of access to which (s) he is authorized, or any attempt to deprive other authorized users of resources or access to any Ashbourne Community School computer system shall be regarded as malicious, and may be treated as an illegal act. The user agrees to be bound by the terms and conditions laid down in the Data Protection Act of 1988 and the Freedom of Information Act of 1997 and to inform themselves of their rights as citizens and their responsibilities under said acts. Other legal / sector specific requirements need to be satisfied under the list of applicable Irish Laws as referenced in this document. All users agree to abide by the terms and conditions of these applicable Irish Laws.

d) **A secure environment**;

- When not in use the doors to the computer rooms must be kept locked.
- All computers in all rooms must be logged off when not in use.
- No user is permitted to use removable storage media that have originated outside of Ashbourne Community School. Storage solutions will be issued by the School, if needed.
- Any user who finds a possible security lapse, or technical difficulty, on any system is obliged to report it to the ICT Development Officer. The system must not be used until the ICT Development Officer has investigated the problem.
- Knowledge of passwords or of loopholes in computer security systems shall not be used to damage computing resources, obtain extra resources, take resources from another user, gain unauthorized access to resources or otherwise make use of computing resources for which proper authorization has not been given.
- Users are responsible for backup of their own data. The ICT Development Officer may from time to time schedule an overhaul and clean up of the network. File owners will be notified of this necessary maintenance, in advance, if such notice is practical.
- All users must become familiar with logging off the system and must do so at the end of every session. If so asked by their teacher, users must ensure that all systems are shut down, though the proper means, when they are finished using them.

6.ACCOUNTS

Accounts will be issued and revoked solely by the ICT Development Officer. Others must not use an account assigned to an individual without express permission from the ICT Development Officer. The individual is responsible for the proper use of the account, including proper password protection. The user is responsible for all work carried out through and transmitted to and from the account issued and for maintenance of files and folders created within said account.

7.CONFIDENTIALITY

Programs and files are confidential unless they have been made available, with written permission, to other authorized individuals. The ICT Development Officer reserves the right to access all information stored on computers other than those used by senior management. File owners will be notified of file access and/or maintenance, in advance, if such notice is practical. When performing maintenance, every effort is made to insure the privacy of a user's files. However, if policy violations are discovered, they will be reported immediately.

8. SYSTEM USAGE
Users must be aware that all their computer activity is tracked and logged for reference purposes. These individual user logs may be accessed at any time by the ICT Development Officer. If policy violations are discovered they will be reported immediately. Electronic communications facilities (such as E-MAIL) are for school related activities only. Fraudulent, harassing or obscene messages and/or materials are not to be sent or stored. The computer facilities may be used during out of class times by any student who has been deemed competent in computer usage by a member of the ICT coordinating committee. Staff may use either of the Computer Rooms with their class group(s) during class time provided the appropriate class period(s) are recorded via the booking procedures in force at that time. Scheduled and timetabled ICT classes take precedence over all other sessions.

9. SYSTEM PERFORMANCE
No one should deliberately attempt to degrade the performance of a computer system or to deprive authorized personnel of resources or access to any school computer system.

10. UNAUTHORIZED ACCESS
Loopholes in computer security systems or knowledge of a special password should not be used to damage computer systems, obtain extra resources, take resources from another user, gain access to systems or use systems for which proper authorization has not been given.

11. COPYRIGHT
Computer software protected by copyright is not to be copied from, into, or by using Ashbourne Community School computing facilities, except as permitted by law or by the contract with the owner of the copyright. This means that such computer and microcomputer software may only be copied in order to make back-up copies, if permitted by the copyright owner. The number of copies and distribution of copies may not be done in such a way that the number of simultaneous users in a department exceeds the number of original copies purchased by that department**.**

12. VIRUS PROTECTION
Computer viruses are items of software that attach themselves to other legitimate items of software or data, without the consent of the computer user, and are programmed to proliferate themselves onto other computers, often to cause disruption or damage. It is essential that all users play a part in protecting the network from the presence of viruses. It is the policy of the school to run up to date virus protection software on all computers that are attached to the network. This software will automatically report the presence of most known viruses. Any user who receives an on-screen warning from this software (these are very clear and explicit) should stop all use of the computer immediately and report the occurrence to the ICT Development Officer or the ICT Technician.
Removable storage media are not allowed to be used in school unless the device has been virus scanned before being connected to any computer on our school network. These must be re-scanned again each time they are used in computers outside the network. Please give reasonable notice to system administrators if scanning is needed.

13. VIOLATIONS
An individual's computer use privileges may be suspended immediately upon the discovery of a possible violation of these policies. Such suspected violations will be confidentially reported to the ICT Development Officer. The Principal may nominate the ICT Development Officer to conduct an examination of computing systems at any time and without prior notice to assure compliance with internal policies, assist with internal investigations, and assist with the management and protection of

the schools information resource systems. Violations of these policies will be dealt with in the same manner as violations of other school policies and may result in disciplinary action. In such a review, the full range of disciplinary sanctions is available including the loss of computer use privileges, dismissal from the school, Garda involvement and legal action. Violations of some of the above policies may constitute a criminal offence.

INFORMATION COMMUNICATION TECHNOLOGY AT ASHBOURNE COMMUNITY SCHOOL
Ashbourne Community School offers timetabled classes for Information Technology in Transition Year, Leaving Cert Applied and Leaving Cert Vocational Programme and all MFL classes. Teachers can book the computer rooms on a daily basis for other year groups. This ensures that all students have access to IT at school. Teachers are encouraged to take their classes to the computer room where the Internet can be used as a virtual library of information. In general classrooms, staff and students have access to a networked PC, data projector, visualiser and speakers. There are two trolleys of netbooks available. One of these is for general use and is stored in RA03 and the other is for for use by LCA and is stored in the Resource Area.

Some teaching staff have access to devices to enhance teaching and learning. A device contract is signed by these teachers

Students have access to Virtual Learning Environments (VLE) in certain subject areas.
An approved VLE is the preferred means of communication between teacher and student. It is much less prone to the abuse prevalent in other social media and provides the necessary framework for teacher-student and student-student interaction in a controlled environment. At the moment Office 365 is the VLE being used in ACS.

Students and teachers work can be saved either to a single server and as a result files are accessible from any computer that is networked or to the students/teachers own One Drive in Office 365

Related school policies:

- Code of Behaviour
- Anti-Bullying
- Child Protection Guidelines
- Data Protection

Legislation

Students, parents/guardians and teachers should familiarize themselves with legislation relating to the use of the internet. The following legislation is available on www.bailii.org or relevant Irish Government sites.

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

Cyberbullying/ Misuse of the internet or of social media

In accordance with the *Anti-Bullying Procedures for Primary and Post-Primary Schools* bullying is defined as follows:

Bullying is unwanted negative behaviour, verbal, psychological or physical conducted, by an individual or group against another person (or persons) and which is repeated over time.

The following types of bullying behaviour are included in the definition of bullying:

- deliberate exclusion, malicious gossip and other forms of relational bullying,
- cyber-bullying
- Identity-based bullying such as homophobic bullying, racist bullying, bullying based on a person's membership of the Traveller community and bullying of those with disabilities or special educational needs.

Cyberbullying is bullying carried out through the use of information and communication technologies such as text, social networking sites, email, instant messaging (IM), apps, gaming sites, chat-rooms and other online technologies. Being the target of inappropriate or hurtful messages is the most common form of online bullying. Cyber-bullying uses technology to perpetrate bullying behaviour and does not require face-to-face contact.

Isolated or once-off incidents of intentional negative behaviour, including a once-off offensive or hurtful text message or other private messaging, do not fall within the definition of bullying and should be dealt with, as appropriate, in accordance with the school's code of behaviour.

However, in the context of this policy, placing a once-off offensive or hurtful public message, image or statement on a social network site or other public forum where that message, image or statement can be viewed and/or repeated by other people will be regarded as bullying behaviour.

Negative behaviour that does not meet this definition of bullying will be dealt with in accordance with the school's code of behaviour.

Reports of cyberbullying will be recorded on a Bullying/Cyberbullying Incident Form and will be dealt with under the Anti-Bullying Policy and the Code of Behaviour.

School's strategies for safe use of the internet

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

AUP Forms

1. All users will be presented with an appropriate acceptable use policy document in line with their role in the school. In August each year, all Staff must sign to acknowledge that they have and accept this AUP document.

   Student AUP forms are in the student journal (see Appendix 5). Once these forms have been signed in the journal, the user will have access to the computing systems in operation throughout the school.

General

2. Present "Cyberbullying, Advice to students: how to stay safe on the internet" (Appendix 1) to all student users.
3. Teach students about the appropriate use of social media
4. Enforce school rules on mobile phones and internet use
5. Make this policy available to parents/guardians and all users on the school website
6. Advise parents/guardians to discuss safe internet usage with their sons/daughters
7. Provide in service training for staff on teaching practice.
8. Ensure Internet sessions are always supervised by a teacher.
9. Use filtering software and/or equivalent systems in order to minimise the risk of exposure to inappropriate material.
10. The school regularly monitors students' Internet usage. All computer rooms including the language lab have monitoring system software such as "AB tutor" for use by the staff in charge of the room.
11. Uploading and downloading of non-approved software is not permitted.
12. Virus protection software is used and updated on a regular basis.
13. The use of personal USB keys in school is not permitted.
14. Staff are given ICT Information and updated guidelines in staff handbook each year and regular emails
15. Students sign in at a computer and sign out when class is finished. This allows the school to know who has worked at any particular computer at any time.

Email

16. Students will use approved email accounts under supervision and only with permission from a staff teaching member and only these accounts must be used when communicating approved work to or from the school.
17. Staff will use approved email accounts when communicating professionally with other partners in education or significant bodies regarding school or educational business.
18. Non school related business will be conducted using a non school email account.

Discussion Forums

19. Students will only have access to discussion forums or other electronic communication forums that have been approved by the school.
20. Discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.
21. Usernames will be used to avoid disclosure of identity.
22. Face-to-face meetings with someone organised via Internet chat are forbidden.

School Website

23. We are privileged to have a portal on the World Wide Web that gives interested parties an insight into the life of the school. This exists at http://www.ashcom.ie. It is envisaged that our students will contribute to the site and they will be given the opportunity to publish projects, artwork or school work on the World Wide Web.
24. The publication of student work will be co-ordinated by a staff member.
25. Students' work will appear in an educational context on Web pages with a copyright notice prohibiting the copying of such work without express written permission.
26. Digital photographs, audio or video clips of students will only be published on the school website with parental/guardian permission(see Appendix 4, agreement form)
27. Personal student information including home address and contact details will be omitted from school web pages.
28. Students will continue to own the copyright on any work published.

Assistive Technology
Appendix 5

Strategies for guiding teacher practice

Teachers in this school:

- Adhere to the Teaching Council's Code of Professional conduct
- Adhere to the school's "staff practice internet use" document (Appendix 3)
- Deliver "Cyberbullying: Advice to students" (Appendix 1)
- Share resources for learning more about cyberbullying and safe internet use (Appendix 2).

User Responsibilities

All users will:

- not visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- be familiar with copyright issues relating to online learning.
- never disclose or publicise personal information.
- 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.
- be aware that use of Internet social network sites such as Facebook, Twitter, YouTube, etc. both inside and outside the school, must not bring the good name of Ashbourne Community School, or any teacher or student of the school, into disrepute. As stated in the school's Code of Behaviour, "Their 'out of school' conduct must not in any way undermine the reputation of the school".
- be advised of the permanent and public nature of posts made on social media and the potential consequences for future career prospects which inappropriate material may represent.

Student responsibilities:

- Students should read and consider the definition of cyberbullying as set out in this document.
- Students should read and consider "Cyberbullying: Advice to students" (Appendix 1)
- Students must sign the AUP form in the Student Journal and agree to comply with this policy.
- Students will use the Internet for educational purposes only.
- 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.
- Students will use approved email accounts for school business only.
- Students will not send or request to receive any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.
- Students will not use removable storage media without permission from a staff member who has had the device scanned for possible viruses.
- Students should report any concerns about internet usage to staff
- Students should report inappropriate material on the web on school computers.
- 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.
- 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.

Sanctions
The aim of this Acceptable Use Policy is to ensure that all users 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 may be withdrawn and appropriate sanctions may be imposed.

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, to involve the Gardai and other legal bodies should the need arise in the case of a serious breach of this AUP.

Circulating, publishing or distributing (including on the internet) material associated with school activities including but not limited to material in relation to staff and students where such circulation undermines, humiliates or causes damage to another person is considered a serious breach of school discipline and may result in disciplinary action.

15. ADDITIONAL GUIDELINES
The ICT Development Officer together with the coordinating committee will establish more detailed guidelines, as needed, for specific computer systems and networks. These guidelines will cover other items related to administration and implementation of a system that offers a first class learning experience to all users.

16. ANNUAL REVIEW
It is envisaged that school and parent/guardian 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.

17. APENDICES
Appendix 1: Cyberbullying Advice to Students
Appendix 2: Internet safety Resources
Appendix 3: Ashbourne Community School: staff practice internet use
Appendix 4: Extract from the school's AUP for Student Journal (including agreement form).
Appendix 5: Assistive Technology Agreement.

This policy has been ratified by the Board of Management of Ashbourne Community School at its meeting on 27th February, 2018. (Ref. Meeting Nr. 231).

Date: _____

Chairperson_____
Board of Management
Ashbourne Community School

APPENDIX 1

Cyberbullying: Advice to Students:
How to avoid trouble

- Never give out your passwords – even to your best friend. Always keep your passwords and PIN numbers to yourself, and make a habit of logging out of your email/Facebook page on your device.
- Choose your friends carefully – remember whatever you post online can be seen by everyone who's got access to your page or the discussion board. If it's Facebook, only make friends with people you're ok sharing information with. Remember, friendships may not be permanent.
- Use Netiquette – be polite to other people online. Think about what you're saying and whether it might be hurtful or might embarrass them in public, even if it's funny.
- Don't send a message to someone else when you're angry – wait until you've calmed down and had time to think. Once you've sent it, you can't take it back.

How to deal with comments or other material that you find upsetting

- Don't reply – even though you might really want to, don't rise to the bait and reply to messages from someone who's bullying you. They want to know that they've got you worried and upset. Chances are if you never reply they'll get bored and leave you alone.
- Go offline – if you feel like it's invading every bit of your life, remember you can turn off your computer and your phone anytime. Ditch virtual reality for some actual reality for a while.
- Inform your Phone Company or Internet Service Provider (ISP) – they can block texts, calls or online messages from specific people.
- Change your contact details – get a new user name, a new email address, a new mobile number and only give them to your closest friends. This doesn't mean you're giving in; you're just getting on with your own life.
- Tell someone – if it's bothering you, don't keep it to yourself. Talk to someone about it. If you're worried your parents/guardians will get angry, you could talk to a friend, or a teacher you trust.
- Inform the Gardaí – if the messages are ever threatening or it's getting really serious. It's against the law to threaten people, and the Gardaí can put a stop to it. They're there to keep you safe, and they generally want to know about stuff like this. Remember also that the Gardaí can trace those who harass others either face-to-face or using communications technology – though they may go to considerable lengths to hide their identity.
- Keep a record (screen grabs/shots, save text messages, etc.) of any material that you find offensive – you don't have to read the messages, but keep them and keep a record of the time and date. This can act as evidence if you ever need it, and can help the Gardaí or your service provider find out where the messages are coming from. Remember, some young people are now using 'chat apps' on their phones and it is not always easy to retrieve evidence without the screen shot – as the images and videos disappear within seconds of being opened.

For more information on what to do about bullying, see the school's Anti-Bullying on the school website or talk to any teacher.

Internet safety resources:

- The Cool School Programme This was developed by the HSE Dublin North East's Child Psychiatry Service and provides an excellent evidence-based overview of the problem, as well practical advice about how to prevent and react to bullying between students in second-level schools.
- A Guide to Cyberbullying Published by the Office for Internet Safety, this guide is clear, comprehensive and easy to understand.
- http://www.internetsafety.ie/ The Office for Internet Safety has been established by the Irish Government to take a lead responsibility for internet safety in Ireland, particularly as it relates to children.
- http://www.webwise.ie An excellent resource that covers much of what schools, teachers and parents/guardians need to know in order to deal effectively with cyberbullying. This site is managed by the NCTE.
- http://www.spunout.ie/health/Healthy-mind/Bullying/Cyber-Bullying
  SpunOut is an independent, youth led national charity working to empower young people between the ages of 16 and 25 to provide an interactive online community for young people to consume health and lifestyle information and find out about health and advice services available to them in their area, online or over the phone.
- http://www.facebook.com/help/325807937506242/ Provides easy to follow advice on how to protect your privacy on Facebook, thus avoiding cyberbullying on Facebook.
- https://www.facebook.com/help/?faq=247013378662696 Clear advice on how to report abusive/inappropriate content on Facebook.
- https://support.twitter.com/groups/33-report-a-violation/topics/122-reporting-violations/articles/15789-how-to-report-violations%23# Advice on what constitutes a violation on Twitter and how to report such violations.
- http://ie.reachout.com/inform-yourself/bullying-and-personal-safety/cyber-bullying/
  ReachOut.com is an Irish service dedicated to taking the mystery out of mental health by providing quality assured mental health information and inspiring real life stories by young people to help other young people get through tough times. ReachOut.com is run by the Inspire Ireland Foundation which is a not for profit, non-government registered charity.
- http://www.socialbrite.org/sharing-center/glossary/
  This provides a glossary of the terms and phrases used in the world of social media. The glossary is constantly being updated to keep pace with developments in the field.
- http://old.digizen.org/downloads/cyberbullyingOverview.pdf
  The information available via this link is a summary of the UK Department for Children, Schools and Families (DCSF) Guidance for schools on preventing and responding to cyberbullying. This document seeks to give practical advice to young people, their parents/guardians and school staff about the issue of cyberbullying. While the information is a little dated, it, it nevertheless, is easy to understand and provides a good overview of the topic.
- http://www.irishtimes.com/newspaper/opinion/2012/1102/1224326036363.html
  This link is to an Irish Times Article 'Education the Solution to Cyberbullying Scourge' by **Dr Sharon McLaughlin,** a lecturer in law at Letterkenny Institute of Technology. Her PhD studies examined child protection in the online environment and she is a member of EU Kids Online network.

- http://www.hotline.ie/ **Irish hotline for reporting child pornography and other illegal content on the Internet.**
- www.watchyourspace.ie **Clear succinct advice on managing children's profiles on social networking sites.**
- EU Kids Online **Hugely informative on the way young people use modern communications technology and contains a specific report on how Irish young people use these technologies and the risks and safety for young people in Ireland using the Internet.**
- How 'Harmless Slagging' leads to cyberbullying. **An interesting Irish Independent Article that includes a short video clip.**
- I was a school bully **– very interesting article in the Journal.ie. The author claims to have experienced both sides of the issue; he bullied and he was bullied. It highlights the importance of pastoral rather than disciplinary approaches to dealing effectively with bullying.**
- Homophobic bullying is a major cause of unhappiness among young people and this **video clip** produced by **BeLonG To** (an organisation for Lesbian, Gay, Bisexual and Transgendered young people, aged between 14 and 23) is an excellent resource in addressing this type of bullying. Each year BeLonG To organise a Stand Up Awareness Week aimed at creating a positive understanding of lesbian, gay and transgender young people and their issues. The 2012 Stand Up campaign was launched by Deputy John Lyons TD – on behalf of the Minister for Education and Skills, Ruairi Quinn.
- The Cyberbullying Virus – a short video that sensitively explores the whole issue of Cyberbullying.
- The father of a young man, who committed suicide after being cyber bullied, tells his son's story and the **pain he has to live with for the rest of his life.**

Ashbourne Community School
Staff Practice: Internet Use

***For the attention of all staff users**

Legislation
Staff members (teaching and non-teaching) should familiarise themselves with legislation relating to the use of the Internet. The following legislation is available on **www.bailii.org** or relevant Irish Government sites.

- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video Recordings Act 1989
- The Data Protection Act 1988
- Section 24.3 of the Education Act

Related school policies:

- Code of Behaviour
- Anti-Bullying
- Child Protection Guidelines
- Data Protection

Teaching Council Code of Professional Conduct for Teachers states:

- **in section 3.7:**
  Teachers should: *'ensure that any communication with pupils/students, colleagues, parents/guardians, school management and others is appropriate, including communication via electronic media, such as e-mail, texting and social networking sites'.*
- ***In section 3.8:***
  Teachers should: *'ensure that they do not knowingly access, download or otherwise have in their possession while engaged in school activities, inappropriate materials/images in electronic or other format'.*
- **In section 3.9:**
  Teachers should: *'ensure that they do not knowingly access, download or otherwise have in their possession, illicit materials/images in electronic or other format'*

School Staff Computer and Internet Acceptable Use Policy

This covers use of digital technologies in school, that is, email, internet, intranet and network resources, learning platform, software, equipment and systems and has been drawn up to protect everyone. The provisions of this policy also apply to access to the internet and email via remote devices such as smart phones and laptops.
Staff are asked to agree to the following:
Usage:

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Principal and the Board of Management.
- I will only use the school's approved, secure email system(s) for any school business.
- I will not allow unauthorised individuals to access email/internet/intranet/network, or other school systems.

- I will not connect a computer, laptop or other device to the network/internet without up-to-date anti-virus software, and I will keep any 'loaned' equipment up to date using the school's recommended system.
- I will use the school's Learning Platform in accordance with school advice.
- I will ensure that any private SNS/blogs, etc. that I create or to which I actively contribute, are not confused with my professional role and are secure against access by uninvited users, that is, students both current and former.
- I will not engage in any online activity that may compromise my professional responsibilities.

Inappropriate material

- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of, inappropriate materials, or filtering breach, to the Principal.
- I will not download any software or resources from the internet that can compromise the network, or are not adequately licensed.

Data and image protection

- I will ensure all documents are saved, accessed and deleted in accordance with the school's data protection procedures.
- I will not use personal digital cameras or camera phones for transferring images of pupils or staff without permission.
- I will not remove any data from the school's system to a storage device or laptop without the appropriate level of data protection and encryption.
- I understand that the Data Protection Policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential.

E-Safety education and students

- I will ensure I am aware of digital safeguarding and internet safety procedures so they are appropriately embedded in my classroom practice.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will report any incidents of concern regarding children's safety to the ICT Co-ordinator or the Principal.

Management and disciplinary procedures

- I understand that all internet usage and network usage can be logged and this information could be made available to the Principal.
- I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action up to and including dismissal.
  (Section 24.3 of the Education Act: Gross Misconduct: Downloading/disseminating pornographic material from the internet; Circulation of offensive, obscene or indecent emails or text messages.)

- I understand that it is my responsibility to ensure that I remain up to date and read and understand the school's most recent AUP.
- I agree to abide by the school's most recent AUP.
- I wish to have an email account; be connected to the intranet and internet; be able to use the school's ICT resources and systems.

Advice for school staff :

- If you discover that arising from your employment as an education professional a website contains incorrect, inappropriate or inflammatory written material relating to you, or images of you which have been taken and / or which are being used without your permission, then this should be immediately reported to Senior Management.
- Senior Management should conduct a prompt investigation.
- If, in the course of the investigation, it is found that a student submitted the material to the website, then that student should be disciplined in line with the school's disciplinary procedures. *Circulating, publishing or distributing (including on the internet) material associated with school activities including but not limited to material in relation to staff and students where such circulation undermines, humiliates or causes damage to another person is considered a serious breach of school discipline and may result in disciplinary action.*
- Where appropriate, Senior Management should approach the website hosts to ensure the material is either amended or removed as a matter of urgency, that is, within 24 hours. If the website requires the individual who is complaining to do so personally, the school should give their full support and assistance.
- If the material is threatening and/ or intimidating, then Senior Management should, with the member's consent, report the matter to the police. Mindful of their health and safety duty of care, management should offer the member of staff support and appropriate stress counselling.

Information Technology Guidelines
Extract from the School's Acceptable Use Policy

(The complete Internet Acceptable Use Policy (June 2014 version) is available on the school website, www.ashcom.ie and copies are available on request in the main office.)

This policy covers use of digital technologies in school, that is, email, internet, intranet and network resources, learning platform, software, equipment and systems and has been drawn up to protect everyone. The provisions of this policy also apply to access to the internet and email via remote devices such as smart phones and laptops.

User definition: A user is defined as an individual who uses a digital device.

Cyberbullying: It is bullying carried out through the use of information and communication technologies such as text, social networking sites, email, instant messaging (IM), apps, gaming sites, chat-rooms and other online technologies. Being the target of inappropriate or hurtful messages is the most common form of online bullying. Cyber-bullying uses technology to perpetrate bullying behaviour and does not require face-to-face contact.

Student responsibilities:

- Students should read and consider the definition of cyberbullying as set out above.
- Students should read and consider "Cyberbullying: Advice to students" overleaf.
- Students must sign the AUP form in the Student Journal and agree to comply with this policy.
- Students will use the Internet for educational purposes only.
- 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.
- Students will not send or request to receive any material that is illegal, obscene, and defamatory or that is intended to annoy or intimidate another person.
- The use of memory sticks in school is not permitted.
- Students should report any concerns about internet usage to staff.
- Students should report inappropriate material on the web on school computers.
- 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.
- 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:

- not visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- be familiar with copyright issues relating to online learning.
- never disclose or publicise personal information.
- 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.

Students:

- are advised that use of Internet social network sites such as Facebook, Twitter, YouTube, etc. both inside and outside the school, must not bring the good name of Ashbourne Community School, or any teacher or student of the school, into disrepute. As stated in the school's Code of Behaviour, "Their 'out of school' conduct must not in any way undermine the reputation of the school".
- are advised of the permanent and public nature of posts made on social media and the potential consequences for future career prospects which inappropriate material may represent.

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, to involve the Gardai and other legal bodies should the need arise in the case of a serious breach of this AUP.

Circulating, publishing or distributing (including on the internet) material associated with school activities including but not limited to material in relation to staff and students where such circulation undermines, humiliates or causes damage to another person is considered a serious breach of school discipline and may result in disciplinary action.

Cyberbullying - Advice to Students:

How to avoid trouble

1. Never give out your passwords – even to your best friend. Always keep your passwords and PIN numbers to yourself, and make a habit of logging out of your email/Facebook page if you're using these on a computer or using these on your mobile phone.
2. Pick your friends carefully – remember whatever you post online can be seen by everyone who's got access to your page or the discussion board. If it's Facebook, only make friends with people you're ok sharing information with. Remember, friendships may not be permanent.
3. Use Netiquette – be polite to other people online. Think about what you're saying and whether it might be hurtful or might embarrass them in public, even if it's funny.
4. Don't send a message to someone else when you're angry – wait until you've calmed down and had time to think. Once you've sent it, you can't take it back.

How to deal with comments or other material that you find upsetting

Don't reply – even though you might really want to, don't rise to the bait and reply to messages from someone who's bullying you. They want to know that they've got you worried and upset. Chances are if you never reply they'll get bored and leave you alone.

Go offline – if you feel like it's invading every bit of your life, remember you can turn off your computer and your phone anytime. Ditch virtual reality for some actual reality for a while.
Inform your Phone Company or Internet Service Provider (ISP) – they can block texts, calls or online messages from specific people.

Change your contact details – get a new user name, a new email address, a new mobile number and only give them to your closest friends. This doesn't mean you're giving in; you're just getting on with your own life.

Tell someone – if it's bothering you, don't keep it to yourself. Talk to someone about it. If you're worried your parents/guardians will get angry, you could talk to a friend, or a teacher you trust.

Inform the Gardaí – if the messages are ever threatening or it's getting really serious. It's against the law to threaten people, and the Gardaí can put a stop to it. They're there to keep you safe, and they generally want to know about stuff like this. Remember also that the Gardaí can trace those who harass others either face-to-face or using communications technology – though they may go to considerable lengths to hide their identity.

Keep a record (screen grabs/shots, save text messages, etc.) of any material that you find offensive – you don't have to read the messages, but keep them and keep a record of the time and date. This can act as evidence if you ever need it, and can help the Gardaí or your service provider find out where the messages are coming from. Remember, some young people are now using 'chat apps' on their phones and it is not always easy to retrieve evidence without the screen shot – as the images and videos disappear within seconds of being opened.

For more information on what to do about bullying, see the school's Anti-Bullying Policy and the school's Acceptable Use Policy on the school or talk to any teacher.

Acceptable Use Policy Agreement Form

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.

Student Signature:_____ Date: _____

Parent/Guardian:
As the parent or legal guardian of the above student, I have read the Acceptable Use Policy and grant permission for my son 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 students access unsuitable websites.

I accept the above paragraph ☐ I do not accept the above paragraph ☐
(Please tick as appropriate).

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.

I accept the above paragraph ☐ I do not accept the above paragraph ☐
(Please tick as appropriate).

In accordance with the Department of Education and Skills guidelines, the school must seek the permission of each student's parents/guardians for use of photographic/video material on the school website and /or for publication that include my son/daughter and allow the school to video record/live stream school events.

I give permission ☐ I do not give permission ☐
(Please tick as appropriate).

Signature:_____Date: _____
(Parent/Guardian's Signature)

Student Name: _____
(IN BLOCK CAPITALS)

APPENDIX 5

Assistive Technology User Policy
Ashbourne Community School

The Assistive Technology User Policy has to be read in conjunction with the Acceptable User Policy (AUP) in Ashbourne Community School. The use of assistive technology by certain SEN students is determined by the NCSE.

Your son/daughter_____, in Class_____has the use of the following:

Equipment:

Software:

Please note that this technology is for the use of your son/daughter during his/her time in Ashbourne Community School. All equipment and software remains the property of either the NCSE or Ashbourne Community School, depending on which organisation has purchased the equipment and/or software. In some instances, the student may use his/her own device – the use of this device is subject to the school's AUP.

Once your son/daughter completes secondary school all School/NCSE equipment must be returned to the SEN Department.

It is expected that your son/daughter will treat and use the equipment and software appropriately, carefully and in keeping with the AUP. Any loss or damage due to mistreatment or misuse will be the responsibility of students and their parent's/guardian's.

Student's Signature: _____ Date: _____

Parent's/Guardian's Signature:_____ Date: _____

Principal's Signature: _____ Date: _____

SEN Department.