 

ACCEPTABLE USE POLICY

BALBRIGGAN COMMUNITY COLLEGE

|  |  |
| --- | --- |
| Document Name | BCC Acceptable Use Policy |
| Version Reference | v.1 |
| Date ratified by Board of Management |  |
| Chairperson of the Board of Management |  |
| Principal/Secretary to Board of Management |  |
| Date for Review |  |

|  |  |
| --- | --- |
|  | A close up of a sign  Description automatically generated |

Table of Contents

[Purpose 4](#_Toc39696572)

[Policy Scope 4](#_Toc39696573)

[Roles and Responsibilities 4](#_Toc39696574)

[ICT Dept. 4](#_Toc39696575)

[Users 4](#_Toc39696576)

[Policy Text 5](#_Toc39696577)

[Principles of Acceptable Use 5](#_Toc39696578)

[Unacceptable Use 6](#_Toc39696579)

[**Passwords and Access** 8](#_Toc39696580)

[**E-Mail** 9](#_Toc39696581)

[**Risks Associated with E-Mails** 10](#_Toc39696582)

[**Bulk Email (Distribution Lists)** 13](#_Toc39696583)

[Internet/Intranet 14](#_Toc39696584)

[Personal Websites 14](#_Toc39696585)

[Use of School Trademark and Logo 15](#_Toc39696586)

[Use of Disclaimer 15](#_Toc39696587)

[Limitations on Uses of Personal Websites 16](#_Toc39696588)

[Student Guidance on Personal Devices and Mobile Phones 17](#_Toc39696589)

[Student Guidance on exempt occasions Personal Devices and Mobile Phones 18](#_Toc39696590)

[Student Guidance on Images and Video 19](#_Toc39696591)

[Student Guidance on Cyber Bullying 20](#_Toc39696592)

[Student guidance on Sanctions 22](#_Toc39696593)

[Supporting Procedures, Policies and or Statutes 23](#_Toc39696594)

[Relevant Policies 23](#_Toc39696595)

[Relevant Statutes 23](#_Toc39696596)

[Breach of Policy 24](#_Toc39696597)

[Review and Approval 24](#_Toc39696598)

[Further Information 24](#_Toc39696599)

[Appendix 1 25](#_Toc39696600)

[Definitions 25](#_Toc39696601)

[Appendix 2 27](#_Toc39696602)

[Sample Letter from BOM 27](#_Toc39696603)

[Appendix 3 28](#_Toc39696604)

[Sample Consent Letters to Parents/Guardians 28](#_Toc39696605)

[Appendix 4 30](#_Toc39696606)

[Reporting Matrix for AUP Policy Breaches 30](#_Toc39696607)

[Appendix 5 31](#_Toc39696608)

[Critical Incident Plan 31](#_Toc39696609)

# Purpose

Providing an efficient and reliable IT service, as well as access to cloud services, to Staff, Students and visitors depends on the cooperation of all Users. It is therefore important that you, as a User, are aware of your responsibilities.

The purpose of this Policy is to provide all Users of the School’s IT Resources with clear guidance on the safe, effective and legal way in which they can use the School’s IT and Network Resources.

By using any of the School’s IT Resources, you agree to comply with the terms of this Policy. This Policy is without prejudice to the right to privacy as protected by the constitution and the European convention on human rights.

# Policy Scope

This Policy covers documentation of policy, procedures, and standards relating to:

* School Information Assets
* School IT and Network Resources

This Policy applies to all Users of the School’s IT resources which includes, without limitation, its networks (accessed on site or remotely) and/or communications devices, other electronic equipment (e.g. photocopiers, cameras, fax machines etc.) hereinafter the School’s IT resources.  This Policy takes precedence over any policies which may be developed at a local level.

# Roles and Responsibilities

## ICT Dept.

The ICT Dept. is responsible for:

* Monitoring use of School IT Resources to ensure this Policy is not breached;
* Acting on breaches to this Policy and bringing any breaches to the attention of the School Principal

## Users

Each User is responsible for:

* Complying with this Policy and all other relevant policies and procedures;
* Ensuring all passwords assigned to them are kept confidential;
* Reporting all breaches of this Policy to the School Principal

# Policy Text

## Principles of Acceptable Use

This Policy is based on the following principles:

All equipment provided by the School for use by staff remains the property of the School. Staff & Students must not remove any such equipment including but not limited to computers, laptops, mobile telephones, etc. from the School premises without prior authorisation from the Principal.

If equipment is removed, loan policies must be followed, and the device must be kept in a secure environment by the user.

It is the user’s responsibility to be informed of the correct operating procedures for the computer resources or products used. A user who is uncertain as to the correct procedure in any situation should obtain clarification before proceeding.

 Users must not engage in conduct that interferes with other’s use of shared computing resources and/or the activities of other users.

1. Users must use the School’s IT Resources and School’s Information Assets in a responsible, safe and lawful manner.
2. Users must respect the integrity of computer systems, communication devices and networks to which they have access.
3. Users must respect the integrity of the data to which they have access.
4. Users must store and process School data in compliance with School policies.
5. Users must follow any standards and guidelines (including those set out in this Policy) relating to the use of the School’s IT Resources and School Information Assets.

## Unacceptable Use

Users are subject to all legislation regulating the use of the School’s IT resources. Users must not store, download, upload, circulate or otherwise distribute material containing:

* Any derogatory comment regarding gender, material status, family status, sexual orientation, religious or political belief, age, disability, race or membership of the travelling community or other categories pursuant to applicable law.
* Any material of a pornographic nature.
* Any material of a paedophilic nature.
* Material containing offensive or foul language.
* Any content prohibited by law.

If an employee receives any offensive, unpleasant, harassing or intimidating messages via e-mail or other computer sources the employee should bring it to the attention of their School Principal.;

Users must not use the School’s IT Resources to:

1. Engage in any form of bullying or other behaviour which is illegal or likely to cause harassment to others.
2. Gain unauthorised access to the account, systems or equipment of any third party - attempts at ‘hacking’ may result in criminal prosecution in Ireland or elsewhere.
3. Use another Users account.
4. Perform any activities which contravene the laws of the State.
5. Undertake commercial activities or to otherwise further commercial objectives which are not a part of your work/studies in the School.
6. Infringe the copyright, patent or other intellectual property rights of any person including, by downloading unlicensed software or other unauthorised materials.
7. Infringe the data protection or other privacy rights of any person.
8. Use of School systems or resource to facilitate plagiarism or cheating in exams or assignments.
9. Access, modify, or interfere with computer material, data, displays, or storage media belonging to the School or another User, except with their permission.
10. Connect unauthorised equipment to the School network.
11. Load or execute unlicensed software or other material on the School’s IT Resources where this is likely to breach the licensing conditions or other Intellectual Property rights.
12. Knowingly introduce any virus, malware or other destructive program or device into the School’s systems or network.

The User should take all reasonable steps to ensure that they do not inadvertently introduce such programs or devices into the systems or network.

1. Store sensitive or confidential School data on personal devices.

If you process (or intend processing) personal data about others on a computer, you are obliged to comply with the provisions of the Data Protection Act 2018 as amended, updated or replaced from time to time and the School’s Data Protection Policy

The School IT resources are to support the activities of the School. Although limited personal use of the School’s IT Resources is allowed, the usage should never conflict with the primary business purpose for which they have been provided and the School’s responsibilities.

In certain circumstances, permission may be given for the use of personal devices. In such circumstances, permission is given on the understanding that the schools bears no responsibility for such devices.

## **Passwords and Access**

Users have a responsibility to safeguard any credentials granted to them by the School. In order to limit security risks, all Users must abide by the following:

* Users must not attempt to bypass or probe any security mechanisms governing access to the computer systems.
* Do not:
* utilise any other person’s access rights or attempt to gain access to resources or data
* Leave their computer unattended without logging out or locking
* misrepresent yourself as another individual. This includes using another staff member’s username and password.
* Passwords must remain confidential to each user and must not be relayed to any other person. The ICT Department may provide the option to alter any passwords as necessary. Each user carries sole responsibility for security access to his/her computer, laptop or any other electronic device.

An approved procedure exists for releasing passwords where accounts are required and staff are unavailable, “Procedure Relating to Access by or Disclosure to a Third Party of Information in a Staff Member's Files or Email Account” : Web & Social Media Policy

The School recognises that the Internet provides unique Teaching & Learning opportunities across a wide variety of social media platforms, such as Facebook, Twitter, YouTube, blogs, etc. However, as the content of such media is largely user-generated, this poses a unique set of legal and reputational risks for the School

The purpose of the [Web and Social Media Policy](https://www.ucc.ie/en/it-policies/policies/sm-policy/#policy) is to inform Staff and Students of the School what the School deems to be acceptable use of these platforms; and to offer Staff and Students a level of protection from any misuse of this medium

## **E-Mail**

Users have an e-mail account to facilitate the sending and receiving of messages for academic and professional purposes. All communications should be done by the organisation e-mail only. While email brings many benefits to the School in terms of its communications internally and externally, it also brings risks to the organisation, particularly where users use it outside of their School roles.

Every user has a responsibility to maintain the School image, to use electronic resources in a productive manner and to avoid placingthe Schoolat risk for legal liability based on their use. It should be remembered that the contents of e-mail are considered as official records for the purpose of legislation such as Freedom of Information Act, National Archives Act, and Data Protection.

The email account of a user, and any information contained in it including content, headers, directories and email system logs, remains the property of the School.

Arising out of the need to protect the School’s network, the School cannot guarantee the confidentiality of information stored on any network device belonging to the School

Email account holders must comply at all times with this Policy

In certain circumstances, permission may be given for the use of personal email for specific activities such as course applications, job applications etc. In such circumstances, permission is given on the understanding that the schools bears no responsibility for such email.

## **Risks Associated with E-Mails**

* Messages can carry viruses that may be seriously damaging to the School systems. To prevent computer viruses being transmitted through the network, care must be taken when dealing with suspect e-mails and attachments of unknown origin are received. Suspect e-mails should be referred immediately to the ICT Dept. and never forwarded to other Users.
* E-Mail attachments may belong to others and there may be copyright implications in sending or receiving them without permission.
* It has become increasingly easy for messages to go to persons other than the intended recipient and if confidential or commercially sensitive, this could be breaching School security and confidentiality.
* E-mail is speedy and, as such, messages written in haste or written carelessly are sent instantly and without the opportunity to check or rephrase. This could give rise to legal liability on the part of the School
* An e-mail message may legally bind the School contractually in certain instances without the proper authority being obtained internally.
* E-mails should be regarded as potentially public information, which carries a heightened risk of legal liability for the sender, the recipient and the organisations for which they work.
* If you receive any offensive, unpleasant, harassing or intimidating messages via e-mail, you are requested to inform the School immediately by <Process?>

 Rules for E-Mail Use

The content of any e-mail must be in a similar style to that of any written communication such as a letter or report as they have the same legal standing. It is important that e-mails are treated in the same manner as any other written form of communication in terms of punctuation, accuracy, brevity and confidentiality.

Similarly, any written, stored or forwarded and disseminated information must adhere to the guidelines within the Data Protection and the Employment Equality legislation and in accordance with the equality policy of the School.

In order to avoid or reduce the risks inherent in the use of e-mail within *DDLETB*, the following rules must be complied with:

* The Schools email disclaimer or a link to same must appear at the end of every e-mail sent from your School address to an external address.
* The school name is included in the address of all staff members and is visible to all mail recipients. This reflects on the image and reputation of the organisation; therefore, e-mail messages must be appropriate and professional.
* Correct spelling and punctuation should be maintained in all communications.
* School e-mail is provided for academic and professional purposes.
* Occasional and reasonable personal use of e-mail is permitted provided that this does not interfere with the administration, teaching & learning and general activities of the School. School email should not be used to support any business and otherwise complies with this policy.
* An e-mail should be regarded as a written formal letter, the recipients of which may be much more numerous than the sender intended. Therefore any defamatory or careless remarks can have serious consequences, as can any indirect innuendo. The use of indecent, obscene, sexist, racist, harassing or other appropriate remarks whether in written form, cartoon form or otherwise is forbidden.
* E-mails must not contain matters which may discriminate on grounds of gender, marital status, family status, age, race, religion, sexual orientation, disability or membership of the Traveller community.
* E-Mails must not contain any inappropriate or lewd content or content likely to cause offence.
* Documents prepared internally for the public or for clients may be attached via the e-mail. However, excerpts from reports other than our own may be in breach of copyright and the author’s consent should be obtained particularly where the excerpt is taken out of its original context. Information received from a customer should not be released to another customer without prior consent of the original sender. If in doubt, consult your manager.
* Do not subscribe to electronic services or other contracts on behalf of the School unless you have the approval of the Principal to do so.
* If you receive any offensive, unpleasant, discriminatory, harassing or intimidating messages via the e-mail system you must immediately inform the Principal.
* Chain mails or unsuitable information must not be forwarded internally or externally.
* Emails should not contain personal information such as addresses, telephone numbers or pictures
* The School reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, received or sent over the electronic mail system for any purpose or where it deems necessary.
* Notwithstanding the Schoolright to retrieve and read any electronic mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorised to retrieve or read any e-mail messages that are not sent to them. However, the confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message.

## **Bulk Email (Distribution Lists)**

In conjunction with the Rules for Email Use, all those who wish to send bulk email to users in the School must comply with the following:

* Take care not to forward emails that were intended only for them to bulk distribution list, such as AllSchoolStudents.
* Chain letters/emails of any sort should not be sent.
* There must be no third-party commercial advertising using school email lists, unless authorised in advance by the Principal.
* Messages originating elsewhere in a private capacity must not be forwarded to the lists without the permission of the original sender.
* Only material in keeping with the purpose of the lists should be sent and, in particular, should not include messages for which other dedicated services are provided.

Replies to this type of message must not be sent to the whole list. Avoid the use of REPLY ALL.

* Messages must be kept as short as possible and must contain only text:
* Images, logos, 'watermark' backgrounds, etc. are not permitted since they greatly increase the size of a message.
* Emails to the list should not include any attachments. Where there is a need to provide staff with copies of reports, forms etc., these should be made available in the cloud and a link to the document included in the message.

In general, messages should be sent only once. Exceptionally, official reminders and security/safety related messages may be repeated.

In the event of an IT Security issue the School reserves the right to stop bulk email lists until the threat has been mitigated.

## Internet/Intranet

The School’s Internet connections are intended for activities associated with:

* The administrative functions of the School;
* The Teaching & Learning activities of the School;
* The professional/academic development of Staff and Students.

Internet/Intranet usage is supervised and may only be accessed with teacher permission.

Internet access and e-mail shall not, for example, be used for the following:

* The Internet must not be used to pay for, advertise, participate in or otherwise support unauthorised or illegal activities.
* To represent yourself as somebody else
* To advertise or otherwise support or engage in illegal activities
* The Internet must not be used to provide lists or information about the organisation to others and/or to send classified information without prior written approval.
* To download pornographic images within view of a colleague or forwarding those images to a colleague, this may result in harassment or sexual harassment.
* To publicise personal information such as addresses, telephone numbers or pictures

The use of File Sharing or Bit Torrent software is strictly forbidden.

Because of the serious criminal implications of accessing child pornography, any user found to be accessing such information may be summarily dismissed or expelled and the matter referred to An Garda Síochána.

## Personal Websites

The School recognises that from time to time Staff or Students of the School will setup websites, blogs or wikis that, while related to their academic or professional disciplines, are personal sites and not formal School sites. The purpose of these rules is to strike the appropriate balance of providing colleagues with the academic freedom to engage in open discourse, while also protecting the reputation of the School and that of its Staff and Students. In addition, these rules ensure that the individual views and opinions discussed openly on such sites are not portrayed as the formal position of the School.

## Use of School Trademark and Logo

Personal websites should not display the School crest, logo or other School trademarked/copyrighted materials, including the School designs, or otherwise appear to be an official School web page, unless with the permission of the Principal.

Personal websites hosted on school or DDLETB infrastructure must not be used for commercial purposes in a way.

## Use of Disclaimer

On personal websites, you are required to identify views expressed as your own and do not hold yourself out as representing the School. If you identify yourself as being a member of Staff of the School, make clear that any views expressed are not necessarily those of the School.

Accordingly, all personal websites created and placed on the School's web servers and/or displaying School or copyrighted material must include the creator's name, and on each page the following statement: 'A disclaimer applies to this page'. The word 'disclaimer' in the statement shall be a link to the following disclaimer:

“This website is the personal responsibility of the person named in the website. Statements made and opinions expressed on personal websites are strictly those of the authors and not the School (“THE SCHOOL”). THE SCHOOL does not preview, monitor, approve or endorse the contents of personal websites, and does not accept responsibility for any loss, damage, harm or injury occasioned by the contents of such websites including, without limitation, content which may be unlawful, offensive, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, discriminatory, libellous, invasive of another’s privacy, hateful or racially, ethnically or otherwise objectionable material or content which otherwise infringes the rights of any third party on any personal page. THE SCHOOL is not responsible for the material contained in, or links connected to, personal websites and cannot be held liable for their contents.”

## Limitations on Uses of Personal Websites

The use of personal websites for the following purposes is strictly prohibited:

* Any use which may have the effect of violating any laws (or exposing the School to unacceptable legal risk).
* Any use which may adversely impact on School computing or on network resources.
* Any use which the School considers may be defamatory or libellous.
* Any use which may infringe the rights of any third party in respect of personal data, intellectual property or other confidential or proprietary information.
* Making accessible materials which could have the effect of damaging the reputation and goodwill of the School.

Are otherwise in breach of this Policy.

These provisions are not intended to curtail the use of Personal Websites.

The School reserves the right to remove personal websites (or links to externally located personal websites) when the limitations set out above are breached or where the staff member resigns, retires or a student graduate or leaves.

Decisions regarding the removal of personal websites and/or links to externally located personal websites for any reason will be made by the Principal, who can be contacted at principal@school.ie . For more information please refer to the Web & Social Media policy.

## Student Guidance on Personal Devices and Mobile Phones

Pupils using their own technology in school should follow the rules set out in this policy, in the same way as if they were using school equipment.

* Pupils are only allowed to bring personal internet-enabled devices into Balbriggan Community College with expressed permission from Managament. i.e for Special Needs students
* Pupils are only allowed to use personal internet-enabled devices during lessons with expressed permission from teaching staff.

Students may carry their mobile phone on their person, but it must be turned off, not on silent.

* The one exception to this rule is during exams, when the Exam Rules will supersede this policy. Mobile phones should NEVER be brought into an exam, and exam papers will be cancelled if it emerges that a student has done so.
* Phones and devices should not be used in any way between or before classes,
* If a student needs to contact home urgently, this will be done through the Main Office. If parents need to contact children urgently, they should phone the Main Office.
* If a student breaches these rules the phone (and SIM card) will be confiscated immediately as per mobile phone policy and given to the Year Head, who will forward it to a member of the School Management Team in keeping with the school’s Positive Behaviour Policy.
* In the event of a dispute about whether these rules have been breached, the phone shall be handed over immediately to the teacher who will give it to the Year Head so the matter can be investigated.
* At all times, the privacy of a student shall be respected. Where the data on a phone is accessed it shall only be to determine whether there has been misuse of the phone, not to monitor the private activities of the owner.

If a phone disturbs a class or if a student is seen using a phone outside the permitted time:

* The phone will be confiscated for 5 school days and only be returned to a parent/guardian.
* A second offence will lead to the phone being confiscated for five days, and will necessitate a parent/guardian attending a meeting after the five days have lapsed.

If a phone has been used to take photographs/audio or video footage:

* The phone will be confiscated until the matter can be resolved.
* If the material has been taken without the consent of the subject(s) therein, the student responsible may be suspended.
* If the material has been taken without the consent of the subject(s) therein and subsequently posted on the internet, shown to others or distributed in any manner, the student responsible may be suspended and may be recommended for permanent exclusion from the school.
* Depending on the nature of the content viewed, Balbriggan Community College reserves the right to contact relevant outside bodies (Gardai, legal advice, HSE, etc) to determine the appropriate course of action.

## Student Guidance on exempt occasions Personal Devices and Mobile Phones

There are certain events in the life of the School where it is normal and reasonable for photographs to be taken and where the explicit consent of the subject therein would usually not be required.

These include, but are not limited to

* Concerts
* sports events,
* TY activities,
* School trips, etc.

Teachers may advise that it is not permissible to take pictures at these events and students must follow this direction. Students should use discretion as to what is appropriate and must continue to be extremely cautious about posting anything to the internet or showing it to others without achieving the direct consent of those involved.

If they are in any doubt at all about what is appropriate, the guidance of a member of staff should be sought in advance. If, in the opinion of the College, their actions are deemed to have been inappropriate the sanctions as outlined above shall apply.

## Student Guidance on Images and Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide opportunities for harassment or breaches of privacy to take place. Digital images may remain available on the internet forever and may cause harm to individuals in the short or longer term.

Care should be taken when taking photographic or video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the College into disrepute.

At Balbriggan Community College pupils must not take, use, share, publish or distribute images of others without their permission.

Taking photos or videos on the grounds of Balbriggan Community College or when participating in school activities is not allowed on personal devices. School devices may be used as part of a Teaching & Learning class or with the express permission of teaching staff. Taking photos or videos the grounds of Castleknock Community College or when participating in school activities is only allowed with expressed permission from staff.

Students must not share images, videos or other content online with the intention to harm another member of the College community regardless of whether this happens in school or outside.

Sharing explicit images and in particular explicit images of pupils and/or minors is an unacceptable and absolutely prohibited behaviour, with serious consequences and sanctions for those involved. Sharing explicit images of other pupils automatically incurs suspension as a sanction.

All parents/guardians are invited to sign the Digital Image Guidelines which grants the College permission to publish photographs of students with due regard to the guidelines.

## Student Guidance on Cyber Bullying

This type of bullying is increasingly common and is continuously evolving. It is bullying carried out through the use of information and communication technologies such as text, social network sites, e-mail, 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. As cyber-bullying uses technology to perpetrate bullying behaviour and does not require face to face contact, cyber-bullying can occur at any time (day or night). Many forms of bullying can be facilitated through cyber-bullying. For example, a target may be sent homophobic text messages or pictures may be posted with negative comments about a person sexuality, appearance etc.

Access to technology means that cyber-bullying can happen around the clock and the pupils home may not even be a safe haven from such bullying. Pupils are increasingly communicating in ways that are often unknown to adults and free from supervision. The nature of these technologies means digital content can be shared and seen by a very wide audience almost instantly and is almost impossible to delete permanently. While cyber bullying often takes place at home and at night, the impact can also be felt in school.

* In accordance with the Counter-Bullying Procedures for Schools, Balbriggan Community College considers that 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.
* When using the internet Students, parents and staff are expected to treat others with respect at all times.
* Engaging in online activities with the intention to harm, harass, or embarrass another pupil or member of staff is an unacceptable and absolutely prohibited behaviour, with serious consequences and sanctions for those involved.
* Measures are taken by Balbriggan Community College to ensure that staff and Students are aware that bullying is defined as unwanted negative behaviour, verbal, psychological or physical, conducted by an individual or group against another person (or persons) and which is repeated over time.

This definition includes cyber-bullying even when it happens outside the school or at night.

* 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 will be dealt with, as appropriate, in accordance with the College’s Code of Behaviour.

In the event of a critical incident please refer to the extract from the “Critical Incident Policy” as outlined in the appendix of this policy.

## Student guidance on Sanctions

Misuse of the internet may result in disciplinary action, including written warnings, withdrawal of access privileges, detention and, in extreme cases, suspension or expulsion. The College also reserves the right to report any illegal activities to the appropriate authorities

Balbriggan Community College will deal with incidents that take place outside the College that impact on the wellbeing of pupils or staff under this policy and associated codes of behaviour and anti-bullying policies. In such cases Balbriggan Community College will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of the College and impose the appropriate sanctions.

Students taking steps to by-pass the content filter by using proxy sites or other means will be subject to disciplinary action, including written warnings, withdrawal of access privileges, detention and, in extreme cases, suspension or expulsion.

Students should immediately report the receipt of any communication that makes them feel uncomfortable is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Balbriggan Community College implements the following strategies on promoting safer use of the internet:

* Pupils will be provided with education in the area of internet safety as part of our implementation of the SPHE and CSPE curriculum. This provision will be presented through the Well Being Programme.
* Internet safety advice and support opportunities are provided to pupils in Balbriggan Community College through our Induction Programme, SPHE Programme (Well Being) & Internet Safety Week
* Teachers will be provided with continuing professional development opportunities in the area of internet safety
* Balbriggan Community College participates in Safer Internet Day activities to promote safer more effective use of the internet
* Sanctions specific to Personal Devices & Mobile Phones are outlined in Section 5 of this Policy and Mobile Device Policy.
* This Policy recognises and respects the importance of The School’s Child Protection Policy in relation to all IT usage & safety

# Supporting Procedures, Policies and or Statutes

The policies and procedures listed in the IT Policies and Procedures section of this Policy provide information or step-by-step instructions on how to implement this Policy.

## Relevant Policies

The Policy should be read in conjunction with other School policies including:

* Code of Positive Behaviour
* Anti Bullying Agreement
* IT Policy Framework
* Web & Social Media Policy
* IT Security Policy
* VLE Policy

## Relevant Statutes

Statutes relating to the use of computers and networking:

* Criminal Damage Act,
* Data Protection Act, 1988
* Data Protection (Amendment) Act 2003
* Child Trafficking and Pornography Act, 1998
* Copyright and Related Rights Act, 2000
* Health and Safety Act (1989)
* Intellectual Property Miscellaneous Provisions Act (1998)
* Interception Act 1993
* Video Recordings Act 1989

Details of these acts can be obtained from;

<https://www.oireachtas.ie>

<https://www.irishstatuebook.ie>

<https://www.oasis.gov.ie>

# Breach of Policy

Any incidents relating to breaches of approved School IT polices will be managed using the IT Policy Breach Handling Protocol defined below.

# Review and Approval

The School reserves the right to amend this Policy at any time in any manner in which the School sees fit at the absolute discretion of the School or the Principal of the School.

Any such revisions will be noted in the revision history of the policy, which are available to you on the school website and by continuing to use the School’s IT Resources following any updated you will be deemed to have accepted the revised terms of this Policy.

**This document requires the following approvals:**

* School Principal
* Board of Management
* DDLETB Director of Schools
* Parents Council
* Students Council

# Further Information

**Contact Email:** info@balbriggancc.net

**Contact Name:** Emmet Sheridan

**Contact Telephone Number:** 01 8412388

# Appendix 1

## Definitions

For the purposes of this Policy, the following capitalised terms (which are used throughout this Policy) shall have the following meanings in the context of this Policy:

|  |  |
| --- | --- |
| Term | Definition |
| Cloud Options | Cloud-based infrastructure includes:* all online programs accessed through a browser
* all applications accessed through a browser

These online programmes and applications that are accessed through a browser include but are not limited to:* Virtual Learning Environments (VLE) such as Schoolwise
* Online platforms such as Google or Office 365
* Social media examples such as Instagram
 |
| VLE | A virtual learning environment (VLE) is a Web-based platform for digital resources and information of school academic activities |
| External Parties | All the School’s subsidiary companies, contractors, researchers, visitors and/or any other parties who have access to the School’s IT Resources. |
| High Severity Incident | An incident that may result in the following.a)   referral under relevant disciplinary procedures for staff or studentsb)   the invocation of the School emergency response plan;c)    a legal action or where there are clear legal implications;d)   warrant a communication plan for internal or external stakeholders.Examples include:a)   abusive email;b)   offensive social media complaint made against a member of Staff. |
| Low Severity Incident | An incident that breached policy but not in a way that is personally damaging to the School or to others.  Examples include:a)   copyright infringement notice;b)   mistaken breach of policy;c)    unwelcome social media comments. |
| Policy | This IT Policy.  |
| Staff | All full-time and part-time employees of the School, including staff recruited for specific purposes. |
| Student | A Student, either full-time or part-time, registered with School. |
| School Information Assets | Information which is of value to the School.  This includes, but is not limited to, information regarding:a)   Students;b)   Staff;c)    financial matters;d)   academic materialThis information may be stored on many different media including:a)   paper;b)   electronic hardware devices (hard drives, flash drives);c)    centrally managed infrastructure including servers and storage;d)   mobile devices;e)   cloud hosted services. |
| School IT Resources | IT resources include those provided centrally by the DDLETB ICT Dept. as well as those provided locally in its offices, departments, schools, colleges or other units.  This includes School IT resources accessed remotely via without limitation:a)   The School’s network and connected networks and to all equipment connected to those networks physically or via wireless.b)   Any networks created independently off the campus network, if they are connected to the School network.c)    All School-owned IT equipment including servers, desktops, laptops, tablets, mobile devices and network-related equipment.d)   Any equipment owned by third parties, leased or personally-owned which use the School network, in conjunction with their work or study in the School. |
| School  | Balbriggan CC |
| Users | All Students, Staff and External Parties. |

# Appendix 2

## Letter from BOM

**Sanctions:**

Misuse of the internet may result in disciplinary action, including written warnings, withdrawal of access privileges and, in cases deemed extreme by the College, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.

This policy has been adopted by the Board of Management of Balbriggan Community College.

**Signed**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Date**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Appendix 3

## Consent Letters to Parents/Guardians



Digital photos and video are exciting new media which can motivate and inspire pupils. Research has shown that using digital images in education can help encourage creativity, motivation and enthuse students and improve communication and team-working skills.

We ask that parent(s) / guardian(s) consent to their son / daughter taking part in the production of digital videos and promotional material. The following guidelines will apply with regard to taking publicity photographs of students in the school,

1. Staff will be aware of possible Child Protection issues when taking photographs of students and where these photographs are used.

2. Parent(s) / Guardian(s) are happy to trust the judgement of teachers in publications such as newsletters, prospectus etc without asking for specific permission each time.

3. Pupils may be identified in these publications to celebrate their achievements.

4. The risks of using digital images in education are minimal but the school has a duty of care towards our students. Therefore pupils in photographs published on our website, www.balbriggancommunitycollege.com will not be named or identified in any way other than by group e.g. Winning Football Team etc.

5. This consent form will apply for the duration of your daughter/son’s time at Balbriggan Community College.

All digital work in the college is underpinned by our Internet Safety Policies.

Please indicate your consent by signing below

Student’s Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Parent(s) / Guardian(s): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Internet Permission Form

Name of Pupil: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Class/Year: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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’s Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

As the parent or legal guardian of the above pupil, I have read the Acceptable Use Policy and grant permission for my son or daughter or the child in my care to access the Internet and to avail of the Windows 365 Platform including the use of Microsoft Teams. I understand that Internet access is intended for educational purposes. I also understand that 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.

 I accept the above paragraph: Yes / No

(Please circle 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 school’s 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: Yes / No

(Please circle as appropriate)

 Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Parent/Guardian)

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Appendix 4

## Reporting Matrix for AUP Policy Breaches

Students are encouraged to reports AUP Breaches while in the school, but outside the classroom as follows;

|  |  |
| --- | --- |
| In Class | Ask the Teacher! |
| Outside of Class |  |
| 1. | Class Tutor |
| 2. | Year Head or Deputy Year Head |
| 3. | Principal or Deputy Principal |
|  |  |

# Appendix 5

## Critical Incident Plan

Social media is now part of everyday communication and information sharing. Most students are avid and competent users. Social media messages speed up the rate at which information is shared. This can have a significant influence on the behaviour of young people during a critical incident. Some social media communication may occur without the knowledge of school staff that leads to distress among students or their parents/guardians.

The following information may assist to consider issues related to social media use when dealing with a critical incident.

* It is essential that the School takes account of the need to have competency in the use of social media among management and staff. If not, the members of the Critical Incident Team should consult those familiar with its use. Senior students from the Student Council could be part of this process. Normalising social media use by the student body during a critical incident is very important.
* Social media literacy should be addressed in the curriculum. It is essential that Schools management, staff and students understand the role of social media, and its positive and negative aspects. A positive disposition to social media by the School may encourage thoughtful use by students during a critical incident.
* Agreement on appropriate use of social media during a critical incident should be included in the School’s Acceptable Usage Policy (AUP). All staff should follow agreed online professional protocols as prescribed by the New Code of Conduct by Teachers i.e. “Teachers should ensure that any communication with pupils/students, colleagues, parents/guardians, school management and others is appropriate, including communications via electronic media, such as email, texting and social media etc.” (The Teaching Council, 2012). The Critical Incident Management Team may also remind staff, students and other relevant community members about their AUP during times of crises.
* When dealing with a critical incident it is advised that the school acts quickly and with caution. A message could be placed on the website and on any other school social media account along the following lines:
* “You may be aware of a recent event within the school community. We ask you to respect the family’s privacy and sensitivities at this time by considering if you should post any comments, especially on social media. We will inform you through the normal channels of any relevant developments”.
* The school could use social media to provide up to date information for all concerned throughout the various stages of the incident. Positive messages and appropriate advice for young people and their parents/guardians to discuss social media use with their children and monitor use more actively following a crisis.
* It is important that the Critical Incident Management Team members are familiar with safe messaging guidelines that should be followed when sending messages to staff. Should the need arise during a crisis; the school’s management can contact the Dublin & Dun Laoghaire ETB for advice and support.
* Young people often post Rest-in-Peace (RIP) messages on social media when tragedies occur. These posts can be heartfelt and emotional particularly in cases of death by suicide. Messages such as “I miss you and will see you soon” or “I will follow in your path” should cause concern and be followed up with the individual concerned. The death by suicide of an individual may influence others. Young people are especially prone to contagion. Those who are emotionally vulnerable may act on suicidal impulses.
* Activity on social networking sites during a critical incident can be a source of potentially important information, such as suicide pacts, identification of vulnerable groups or individual young people who may be at risk of suicide. Given privacy restrictions to people’s personal pages, distressing information may be posted without the knowledge of parents/guardians or School management. It is likely that users will block access so activity of this nature will not be accessible to everybody.