



BLESSED TRINITY COLLEGE

ICT Acceptable Use,
eSafety & Device Policy
(Students)

SEPTEMBER 2021

TABLE OF CONTENTS

RATIONALE	3
PURPOSE	3
COLLEGE FACILITIES.....	4
ELEARNING RESPONSIBILITIES AND EXPECTATION	5
ESAFETY.....	6
PERSONAL DEVICES.....	7
ACCEPTABLE USE POLICY – STUDENT AGREEMENT FORM.....	9

RATIONALE

New technologies have become integral to the lives of learners in today's society, both within Blessed Trinity College and in their lives outside of the college. The internet and internet connected devices are powerful tools, which open up new opportunities for learning. These technologies can inspire discussion, promote creativity and stimulate awareness of context to promote effective learning for students. They also bring opportunities for staff to be more creative and productive in their work, continuing and enhancing the learning and teaching experience beyond the classroom.

Blessed Trinity College is committed to ensuring learners understand how to use the hardware and software available to them, how to keep safe and act responsibly when accessing the internet and devices whilst in and out of school. The college will ensure each learner is provided with information regarding how to keep safe and behave appropriately whilst online, and how to report concerns they might have through a broad range of eSafety advice and training.

While recognising the benefits of ICT, internet connected devices and social media, this policy sets out the principles that students are expected to follow when using ICT facilities in college to access the internet, as well as smart phones and other connected devices. Students are expected to behave online in a way that does not compromise their own safety, the safety of others, or the reputation of the college.

PURPOSE

This policy document is intended to ensure:

- that students are responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that college ICT systems and student users are protected from accidental or deliberate misuse that could put themselves, the security of the systems and the safety of other users at risk.
- that students are protected from accidental or deliberate breach of the College's Safeguarding and Child Protection Policy, regarding their own and other students' welfare.
- that potential issues involving smart phones and other connected devices can be clearly identified and addressed.

COLLEGE FACILITIES

Learners have access to a range of devices including PCs, laptops and iPads in school. As well as this, they have access to services like Office365 and Google Classroom while at home to allow for work to be continued and completed remotely. The students' C2k log-in details can be used to access these services.

Students are asked to respect all the ICT facilities in the college and not to use these facilities for non-educational purposes or to damage college property, this includes disconnecting hardware. If learners identify damaged equipment, it should be reported immediately to the class teacher.

Passwords

A password will be provided to learners at the start of the autumn term, allowing them to access C2k devices and programmes like Office365 and Google Classroom. The learner is required to change this password to something memorable. This password should never be shared with others and can be used to access the network while in college and at home. Students should never try and access the accounts of others either to cause damage or to download work, this is a breach of the college's Acceptable Use Policy (and the Computer Misuse Act 1990), and could see sanctions being carried out.

Managing Email Accounts

BTC will provide all students with an official email address (@c2ken.net). This address is the only one which should be used for college communication (email can be monitored by staff). Students will be made aware of the appropriate use of email. They will also be advised to be careful with whom they share this email address. Students are advised that this email address should only be used for college related activities and that it is not private.

The email addresses may be used to allow students to access services which the college has deemed as appropriate for use within school (e.g. cloud-based storage and associated applications like Google Classroom). Use of email accounts and any services accessed using that account will only be used in accordance with the current college guidelines.

Use of the Internet

All internet access provided within the college is filtered by C2k. Access to websites with inappropriate content is monitored by the provider, blocked and reported. Students should use this internet for access to educational sites only, other sites should only be accessed under the direction of the class teacher. Online gaming, social media and video streaming are blocked and should not be accessed, students should not attempt to access services to bypass this filtering system. If students do not follow the guidelines, internet access on their accounts can be blocked by the administrator, if required.

ELEARNING RESPONSIBILITIES & EXPECTATIONS

eLearning is used to enhance and extend classroom teaching, for the completion and submission of homework, assignments and to support learners whilst working from home during periods of remote learning such as illness, or extreme weather conditions.

- As per Blessed Trinity College expectations and core values, you must always be respectful to your teachers and fellow students when communicating electronically.
- You are not to record or forward any content within our eLearning platforms – such as worksheets, exam papers, answers, solutions, videos, notes or Google Meet links – to anyone else without the permission of the creator of that content.
- You understand that all your online activity is recorded; this includes anything you send or say via email, on the Google Classroom Stream or in a Google Meet.
- When completing work electronically, it is important you follow copyright law and all work you submit is yours. Teachers have access to plagiarism software, any violations will be reported to the Head of Year, and for exam year students reported to the examination body, as per normal procedures.

For Parents/Carers:

- You should ensure that your child is checking in regularly for assigned work.
- Where live classes are being run, please try to arrange that your son/daughter is in an area of the home that is quiet and free from distractions. Please be mindful of Child Protection Guidelines, for example, bedrooms should not be used for live classes.
- Live online classes should be viewed by your son/daughter only.

Live Online Classes

Teachers may deliver some of the course “live” using Google Meets (or other alternative video conferencing applications). This will use varying combinations of audio, video, virtual whiteboards and screencasts. In the use of Google Meets:

- Students must always follow the direction of their teacher, just as in the classroom.
- Students are not to turn on their camera or their microphone, unless the teacher invites them to do so.
 - In any case, all microphones should be on mute when a person is not speaking, to avoid distracting background noise being broadcast to everyone.
- A Google Meet link is intended for the student only; the teacher will decide who should receive the link, do not forward any link to anyone else.
- All Google Meet sessions are recorded, and these recordings may be made available by the teacher to the class to watch back again later. This recording includes any video, screenshares, whiteboards and audio from the class.
 - Students are not to share these recordings with others.
- Only the teacher is allowed to record a session; no-one else is permitted to record.
- Any students who do not follow the agreed procedures for online lessons may be removed from the Meet.

eSAFETY

All learners must read and sign the acceptable use policy before being given access to our computer network, IT resources or internet. As well as this, the college will deliver an age appropriate eSafety programme and promote events such as Internet Safety Day in order to show students how to protect themselves online and take responsibility for their own and others safety.

Filtering & Monitoring

Levels of Internet access and supervision will vary according to the student's age and experience while in Blessed Trinity College. Online content learners have access to is closely monitored, and anything that is regarded as inappropriate or not suitable for school will be blocked. The IT technician, in consultation with senior and middle leaders, will manage the configuration of the filtering system to ensure that it is appropriate, effective, and reasonable. The college will report any online material it believes to be illegal to the appropriate agencies.

Social Media

Expectations regarding safe and responsible use of social media applies to all members of the college community. The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messaging platforms. All members of the college community are expected to engage in social media in a positive, safe and responsible manner. The college's filtering and monitoring system will control student access to social media while using college provided devices and systems on site.

Safe and appropriate use of social media will be taught to students as part of an embedded and progressive education approach, via age appropriate sites and resources. Any concerns regarding a student's use of social media will be dealt with in accordance with existing policies. Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

Students will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
- To only approve and invite known friends on social media sites, and to deny access to others by making profiles private.
- Not to meet any online friends without a parent/carer's permission, and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age, stage and ability.
- How to block and report unwanted communications.
- How to report concerns both within the setting and externally.

PERSONAL DEVICES

The college recognises that many parents/carers may wish their child to have a smart phone (or other personal electronic devices) for use in cases of emergencies. The college reserves the right to confiscate a student's smart phone (or other devices) if it is used inappropriately.

PROCEDURES IF DEVICES ARE OBSERVED DURING THE SCHOOL DAY

- In the 1st instance, a smart phone/device will be confiscated by the teacher and taken to reception for storage. The student can collect the phone at the end of the school day.
- In the 2nd instance, a confiscated smart phone/device will only be returned to a parent/carer by appointment with the Head of Year.
- In the case of repeated instances and a blatant disregard for the policy guidelines, a confiscated smart phone/device will only be returned to a parent/carer by appointment with the Year Group Assistant Vice Principal.
- It should be noted that the College will report any matters to the police which are subject to illegal misuse of smart phones, social media, or ICT facilities, in relation to school.

The use of smart phones during the college day to make telephone calls, send or receive SMS/IM, take photographs or listen to music (this list is not exhaustive) is restricted with devices being switched off at ALL TIMES, including between classes, breaktime and lunchtime, unless directed otherwise by staff.

Exceptions may be permitted only in exceptional circumstances if the parent/carer specifically requests it. Such requests will be handled on a case-by-case basis, and should be directed to the appropriate Head of Year. Parents/carers are reminded that in cases of emergency, the college office remains the appropriate point of contact and can ensure your child is reached quickly and assisted, as appropriate.

- The misuse of smart phones and other personal electronic communication equipment for cyberbullying will not be tolerated.
- Staff discretion is advised when asking students to engage in any activity which would require them to use personal devices. Students will be advised as to what is appropriate and inappropriate in these circumstances.
- In accordance with JCQ regulations, phones and devices must not be taken into examinations. Students found in possession of a smart phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

- Students should protect their phone number by only giving it to trusted friends and family members. Students will be instructed in safe and appropriate use of smart phones and personally owned devices, and will be made aware of boundaries and consequences.
- It is forbidden for students to use their smart phones/other devices to take videos and pictures of other students or staff without their consent and then send the pictures to other students or staff or upload it to a website for public viewing.
 - It is a criminal offence to use a smart phone/internet to menace, harass or offend another person and almost all calls, text messages and emails can be traced.
- Smart phones/other devices are not to be used in changing rooms or toilets or used in any situation that may cause embarrassment or discomfort to their fellow students, staff or visitors to the college.

If there is a circumstance when smart phones or devices are required to be switched on, then;

- The Bluetooth function must be switched off and not used to send images or files to other devices.
- Devices should be silenced and must not disrupt classroom lessons with ringtones, music, or beeping.

Loss, Theft or Damage

Students should mark their device clearly with their names. Smart phones/other devices that are found in the college and whose owner cannot be located should be handed in at reception. The College accepts no responsibility for replacing lost, stolen or damaged smart phones/devices. The College accepts no responsibility for students who lose or have their smart phones/devices stolen while travelling to and from school.

It is strongly advised that students use passwords/pin numbers to ensure that unauthorised access/phone calls cannot be made on their college login account or smart phones (e.g. by other students, or if stolen). Students must keep their password/pin numbers confidential. Smart phones and/or passwords should not be shared.

ACCEPTABLE USE POLICY – STUDENT AGREEMENT FORM

I understand that I must use college ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the college will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating online.
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc).
- I will not arrange to meet people offline that I have communicated with online without parental knowledge.
- I will immediately report any unpleasant or inappropriate material or messages, or anything that makes me feel uncomfortable when I see it online.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the college systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use, unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the college systems or devices for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act towards me:

- I will respect others' work and property, and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language, and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the college has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the college:

- I will only use my own personal devices (smart phones / USB devices etc) in college if I have permission). I understand that, if I do use my own devices in the college, I will follow the rules set out in this agreement, in the same way as if I was using college equipment.

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not install or attempt to install or store programmes of any type on any college device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information I access is accurate, as I understand that the work of others may not always be truthful, and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of college:

- I will follow all BTC eLearning responsibilities and expectations outlined in this policy.
- I understand that the college also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of college and where they involve my membership of the college community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the college network / internet, detention, exclusion, contact with parents/carers, and in the event of illegal activities involvement of the PSNI.

Please complete the section below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement.

Student's name _____ Class _____

Student's signature _____

Parent/carer's signature _____ Date _____

* Parents/carers are advised not to post pictures of students on social networks or post malicious/fictitious comments regarding our college community. Parents should make complaints through official channels.

