



Technology Enhanced Learning Acceptable Usage of Digital Technologies & Internet Policy 2024/25

John the Baptist Community School

Rationale for Digital Technologies Acceptable Usage Policy

The aim of this Acceptable Usage Policy (AUP) is to ensure that students will benefit from learning opportunities offered by the school's Digital Technology resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. If the school AUP is not adhered to, this privilege may be withdrawn, and appropriate sanctions imposed.

It is envisaged that school and parent/guardian representatives will be involved in the review of this policy on a regular basis.

Mission Statement

John the Baptist Community School is committed to the provision of a broadly based education in an atmosphere of mutual trust and respect, balancing vision with realism, which facilitates personal growth and development among students, staff and community, within the context of a Christian ethos.

School's Vision for Technology Enhanced Learning

Our school recognises the importance of integrating Digital Technology into learning and teaching in order to equip and prepare our students to live and work in a 21st Century Society. Our eLearning mission statement reads as follows:

John the Baptist Community School is committed to realising the potential of digital technologies to enhance and deepen teaching, learning and assessment so that our students can develop a set of broad transferable skills which enable them to participate fully in modern 21st century society and the economy.

In order to achieve this, we must provide suitable structures, resources and skilled personnel to ensure that our students have the opportunity to develop a range of key skills throughout their post-primary school journey. We must endeavour to ensure that at the end of the Senior Cycle, students have acquired key skills and a solid foundation of Digital Technology competencies that will support their learning and transition to further or higher education.

To realise this vision, it is important to recognise the role of students, teachers, school leaders and parents/guardians. Future planning in this area will involve the engagement of all stakeholders.

Students

- Use ICT to access and engage with new forms of learning and collaboration to support different styles of learning.
- Experience the benefits of using digital technologies which may increase engagement and levels of success in their education and lifelong learning.
- Actively engaged in learning – both in and out of school.
- Accept ownership of their learning – involving the ability to be self-directed, a decision maker and a manager of priorities in and out of school.
- Use digital technology to achieve personal learning goals and to succeed in various learning activities.
- Use Digital Technology critically, ethically and responsibly. (AI policy in progress, see Counter bullying policy)

Teachers/Staff

- Facilitate the use of digital technology in the classroom and at home providing student-centred guidance and feedback. This encourages engagement in exploratory and collaborative activities with students.
- Using ICT to “support an enquiry process and enable their students to work on solving complex real-world problems” by engaging in “collaborative project-based learning activities that go beyond the classroom”
- Support students to create and innovate so that they are engaged in managing their own learning goals and activities.
- Accept ownership of their own professional learning and, where appropriate, designing and participating in learning communities that make extensive use of technology.

School Leaders

- Take a lead role in planning how they will effectively embed ICT in teaching, learning and assessment practices. This means involving the entire school community in developing an e-Learning plan that takes into account the CPD needs of teachers, and the views and insights of students and parents/guardians.
- Developing policies and practices for the safe and ethical use of ICT by all members of the school community.
- Strengthening their existing relationships with the wider community, both local and global, and, in particular, connecting more with parents/guardians and students in their homes through the use of digital technology.
- Collaborate with digital leaders from other schools and organisations to inform best practice.

Parents/Guardians

- Engage with their children’s learning through the use of digital technologies.
- Collaborate with and participate in school activities and programmes using ICT.
- Have read in full all aspects of the school’s AUP and discuss in depth with their student
- Take an active role in their student’s digital learning
- Endeavour to monitor, educate and raise awareness with their student concerning internet safety, best behaviour online and etiquette surrounding digital interactions

Digital Technologies Covered in this Policy

John the Baptist C.S. may provide students with internet access, access to desktop computers, digital imaging equipment, laptop or tablet devices, video-conferencing capabilities, virtual learning environments, online collaboration capabilities, online discussion forums, email and more. As new technologies emerge, such as

those apps and extensions used in remote learning experiences, John the Baptist C.S. may provide access to them also. The policies outlined in this document are intended to cover all online and offline technologies used in the school, not just those specifically mentioned. As new technologies are incorporated into John the Baptist C.S., this policy may be updated accordingly.

Computer and network resources are powerful technologies for accessing and delivering information and knowledge. As such, they are strategic technologies for the current and future needs of the school. Because these technologies give individuals the ability to access and copy information from remote sources, users must respect the rights of others, respect the integrity of the systems and related physical resources, and observe all relevant laws, rules, regulations and contractual obligations. These will include all of the school's existing regulations and policies. This policy applies to all staff and to others who are authorised to use the computer and network resources. The policy also applies to all computer and network facilities controlled or contracted by the school. These include teacher devices, computers, workstations, servers, communication equipment as well as associated peripherals and software regardless of whether used for administration, teaching, training, research or other purposes.

Access to John the Baptist C.S.'s Internet Network

John the Baptist C.S.'s internet network is intended for educational purposes only. Access to ICT is considered a school resource and a privilege. The school's computer and network resources represent a considerable investment and providing access to them is expensive. Therefore, if the school AUP and by extension all school rules not adhered to, this privilege will be withdrawn and appropriate sanctions, as outlined in this AUP, will be imposed.

- Students are expected to follow the same rules for good behaviour and respectful conduct online as offline – these rules are found in John the Baptist C.S.'s Code of Behaviour.
- All activity over the network may be monitored and retained.
- Access to online content via the network is restricted and filtered in accordance with our policies and the policies of the Department of Education and Skills through its agency, the National Centre for Technology in Education. Users are expected to respect that the web filter is a safety precaution and should not try to circumvent it when browsing the web. If a site is blocked and a user believes it shouldn't be, the user can ask management to submit the site for review.
- The school's systems should not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive codes such as viruses, self-replicating programs, inappropriate or derogatory text or images, or any other unauthorised materials. (See Counter Bullying policy)
- Proxy servers are strictly forbidden. Any attempt to circumvent the internet filtering system is a serious breach of this AUP.

- Under no circumstances should students access or attempt to access the teacher WiFi network on a personal device.
- Students should report accidental accessing of inappropriate materials on the internet immediately to the teacher present.
- Users should not engage in any activity online which is in breach of local, national or international law.
- Users shall not use the school's internet connection to download unauthorised software, "plug-ins", games or other entertainment software (including screensavers) or save inappropriate or offensive material.
- Users should not engage in any activity online which is disrespectful and may bring John the Baptist C.S., its staff or student body into disrepute.
- Misuse of school resources for purposes other than those set out by a teacher/staff member or a school activity, will follow appropriate sanctions as outlined in this policy.
- A student is expected to alert his/her teacher immediately of any concerns for safety or security.
- Students should not copy information into assignments and fail to acknowledge the source (plagiarism and copyright infringement). AI policy in progress.
- Students will only have access to chat rooms, discussion forums, messaging or other forms of electronic communication that have been approved by the school. Relevant sanctions outlined in this policy will be imposed for any attempts to access, establish or use any other online communication forums. The Office 365 platform has been established in order to provide a safe, secure and monitored environment for school communication.

John the Baptist Community School will make every reasonable effort to ensure students' safety and security online but will not be held accountable for any harm or damages that result from misuse of school technologies.

Office 365 Usage

John the Baptist C.S. provides students with Office 365 accounts for the purpose of Technology Enhanced Learning. This is a secure, dynamic, collaborative, purpose driven platform which provides students with opportunities for personalised learning, deepening their understanding of the curriculum, and the development of 21st Century future ready skills. It also facilitates a broader range of assessment approaches which are appropriate to a wider range of learning experiences and styles. To ensure that all users on the Office 365 system can benefit fully from the experience it provides, student are reminded that its availability and use is in line with school policies such as the Code of Behaviour, Child Safeguarding Statement, the Counter Bullying Policy and the Data Protection Policy & Data Retention schedule. Furthermore –

- John the Baptist C.S. recognises that online collaboration is essential to education and may provide students with access to a variety of online tools that allow communication, sharing, and messaging among students and teachers.
- All forms of communication across the Office 365 platform must be respectful, mindful, and courteous and for **school related purposes** only. This includes but is not limited to, emails, collaboration spaces (e.g. on One Note) and post threads on Teams. Any communication including email may be monitored and archived at any time. Students should not under any circumstance use their school account to sign up or subscribe to nefarious inappropriate online sites, chatrooms, mailing lists or organisations etc. This opens the school and its online systems to possible breach and degradation. Sanctions may apply to anyone doing so, up to and including suspension and expulsion.
- Educational programmes are in place which instils in students the safe practice and ethical use of digital technologies. It is envisaged by the school that this platform is used in a manner that reinforces and embeds these safe practices. The school takes part in the annual Safer Internet Day (February) with a series of in-class presentations, shared links, presentations, quizzes and information sessions.
- Students will not send or receive any material that is illegal, obscene and/or defamatory, or that is intended to annoy or intimidate another person. Any such actions may result in the school contacting law enforcement and other relevant national agencies such as TUSLA.
- Materials saved by students on this platform using apps such as Teams and OneDrive should be school related only. Material such as photos should not contain imagery or data that is inappropriate or unrelated to schoolwork.
- Inappropriate images used as avatars or profile pictures will be removed and the student may face sanctions.
- No unauthorised guests are allowed on our school Microsoft platform to maintain its integrity
- Teachers are the owners/ managers of the Teams they create. Most Teams will be whole class groups but this may vary. When students are invited onto and put into a Team it is the exact same as being in the classroom and being with a class group. They have a teacher and the school's same rules continue to apply. Students do not have permission to create Teams.
- The chat function is not available between students at present to maintain safe, monitored communication between students at all times.
- Students will be added to Teams as teachers deem appropriate. Students are not allowed to leave a class once added by a teacher. Students should note that teachers, SNAs and student teachers may have admin access over a given Team as needed to facilitate deep learning and collaboration.
- The use of emails must be careful and measured. No sensitive data should be shared by email. The opinions expressed in an email may not reflect that of those of the school. If a user receives an inappropriate email or sends an email in error, they should inform the school immediately. Teachers should not be contacted directly through their school email.

- Student email accounts are closed after the cessation of their studies at the school with a grace period of 6 months from their last day of school.
- Sixth Year students should be aware that their 365 accounts are closed at the end of the calendar year in which they finish their studies at John the Baptist C.S. They are notified of this via Teams hub and a text home approximately one month before finishing school.

Cyber-Bullying

The Department of Education and Skills defines cyberbullying as; “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.” Harassing, ‘flaming’, denigrating, impersonating, outing, tricking, catfishing, gas lighting, phishing, fraping, excluding and cyber-stalking are all examples of cyberbullying.

- Such bullying will not be tolerated in John the Baptist C.S. Please see John the Baptist C.S.’s Counter-Bullying Policy.
- Inappropriate actions on social media sites can also constitute bullying, e.g. “liking” degrading comments/photos on Facebook, trolling etc.
- THINK.... Don’t be mean. Don’t send emails or post comments or photos with the intent of scaring, hurting and/or intimidating someone else.
- Engaging in any online activities intended to harm (physically or emotionally) another person, will result in disciplinary action and loss of Digital Technology privileges.
- In some cases, cyber-bullying is a crime and may be reported to the Gardai.
- Students are advised that activities are monitored and retained.
- The school will support students, teachers and parents in dealing with cyber-bullying.

Social Media

The use of social media is widely pervasive within society. The misuse and abuse of social media can be a source of much worry, harm and danger for all. Social media sites/apps such as Facebook, Snapchat, Instagram, TikTok etc. are not accessible with the school’s Wi-Fi system for any users. While infringements and issues using social media may occur outside school, the school reserves the right to intervene, investigate and address any such issues, e.g. those involving such as cyber-bullying, that may directly impact negatively on members of the school community and have a damaging impact on learning and teaching in the school. Such incidents will be dealt with in accordance with the school’s Counter Bullying Policy as well this policy and may result in serious sanctions.

All users should be aware that as per the school's Code of Behaviour, sexting is the sharing of sexual text, video, and photographic content using mobile phones, apps, social networking services and other internet technologies. The sharing of explicit text, images and/or video is an unacceptable and absolutely prohibited behaviour and will have serious consequences and sanctions for those involved in accordance with the school's Code of Behaviour. All incidents involving creating, storing, or sharing of explicit text, images and/or video of children under the age of 17 years will be reported as an incident to the Gardaí and Tusla and the State Claims Agency (to the latter as there is the potential to cause injury/harm to the individual). Sharing of explicit text, images and/or videos of pupils in the school will incur serious sanctions including suspension and up to expulsion as determined by the Board of Management.

Social media platforms are not suitable for learning and teaching activities. The school employs the use of a secure school website and official school X (formerly Twitter), Instagram and Facebook accounts for PR and communications purposes. These are administered by limited dedicated individuals within the school and used for promotion, information and display purposes only. The website and social media platforms will be regularly checked to ensure that there is no content that compromises the safety or personal data of students or staff. It will also be checked to see that no content denigrates an individual or might threaten the good name of the school and that the language and tone used is appropriate.

Parents/Guardians are asked not to contact teachers/staff or school through any form of social media. If a parent/guardian wishes to contact a staff member, they should do so through the main school account during school hours info@johnthebaptistcs.ie

Students should not contact, attempt to contact or follow/join a teacher's personal social media account under any circumstances, to maintain the professional and respectful relationship vital for school life. Such an attempt or the sending of unsolicited messages will be seen as inappropriate and as a direct contravening of this policy and will incur serious sanctions, up to and including suspension and expulsion, depending on severity.

Unauthorised access to a school account

Every effort must be made by all users to keep the login details and password of their school account safe and secure. The sharing of such information, both intentionally or by accident, can have serious repercussions and will face sanctions, up to and including suspension and expulsion.

Identity Theft

Only a school account should be used by students and staff for school communication. Users must not send anonymous emails. Using the email address of another user to send an email is also prohibited. All users are reminded to log out of any device they may use. If a user becomes aware of another's account open on a

given device, they should log out immediately. The viewing of any material associated with the account will be considered a data breach and will be reported to the Data Protection Commissioner and may result in serious sanctions and a fine. Any use of another's account will be considered identity theft and can be reported to Gardaí.

Identity theft is a serious crime. Any student who gains, retains or uses the personal identifying information of any member of the school community, such as that of a member of staff or student, may face serious sanctions. This includes impersonating a member of the school community and using images or information to set up a fraudulent account on any form of social media. John the Baptist C.S. is committed to making the online experiences of our students and staff as positive and as secure as possible. If a member of the school community becomes aware of an account set up in their name or using their data such as image or that of another, they should inform the school and Gardaí immediately. The use of the name of a member of our school community to perpetrate a crime or an inappropriate act is not acceptable. The school will make every effort to clear the good name of those involved and seek to bring perpetrators to justice.

Passwords and Hacking

All online systems are susceptible to infiltration and unauthorised access. Careful managing and control of one's information and details can greatly limit this issue. Users are reminded to not share their account details or password with others and to follow these guidelines when choosing a password. A new password must:

- Be 8 characters in length
- Have at least one capital letter
- Have at least one lower case letter
- Have at least one number
- Not use your name or identifying information

Please note that for data protection purposes, the school can never see a user's password and it can only be reset if lost/forgotten by an administrator. A new section was added to the school journal in 2020/21 to remind students of key points (see Appendix 4). Passwords should never be written down and left in a location easily accessible or visible to others. This includes both paper and digital formats on untagged (unsupported) devices. Passwords should not be stored in a web browser's password manager on an untagged device. Users should make every effort not to leave themselves logged into an application or system where someone else can unknowingly use their account

If a school user becomes aware that their account or that of someone else may have been compromised, they are asked to immediately report it to the school. The account will be immediately blocked. The named owner of the account will not have access. An investigation will then occur which may include some or all of

the following: staff members, students, parents/guardians, the Digital Learning team, school management, outside experts, Microsoft, internet suppliers and the Gardaí.

Users should be aware that all activity is monitored, including the IP addresses of logins to ensure the continuity and safety of this vital online learning resource. The school reserves the right to fully investigate all reported incidents of hacking or unauthorised access. During this time, the account of the owner may not be available. Staff will be informed of such, and alternative arrangements for accessing online materials may be made.

General Procedures and Practices for the use of Digital Technologies in Computer rooms and when using Laptop Trolleys

- Open internet sessions will always be supervised by a teacher. No student has access to a computer or school device without teacher supervision.
- Students must be assigned a laptop number/ computer as documented in a classroom seating plan.
- Unauthorised/ inappropriate use of web cams and/or integrated cameras within devices is strictly forbidden. Recording of unauthorised material and/or persons is strictly prohibited and sanctions will apply.
- Students must respect the physical nature of all equipment, including keyboards, central processing units (tower), mouse and desktop monitors. In particular, any attempts to alter the configuration of keys on the keyboard or remove or alter any mouse is viewed as grave misconduct and an act of vandalism and sanctions may apply.
- Food and drink are forbidden in all computer rooms as well as in classrooms where digital devices are being used. Students should take care to log out of all accounts and shut down digital devices after use.
- Laptops used from a trolley should be returned to the correct shelf and plugged in at the end of class.
- Laptops are not to be taken from the trolley on an individual basis unless the whole trolley is book.
- Computer rooms should be left neat and tidy.
- It is forbidden to move input/output devices such as printers, computer mice and keyboards from their fixed location, i.e. between devices or from room to room.
- All issues with Digital technology should be reported to the teacher.
- Each student will be issued a unique email. This will grant them access to their own office 365 account. Students should always only use their own account. This account should be used for educational purposes only.
- Students will be provided with training on how to log in to their Office account and how to send emails appropriately with the correct etiquette. This will be done through a Digital learning class in first year and/or support videos online.
- Uploading/downloading and installation of non-approved software is not permitted.

All relevant requests must be made to the ICT coordinator in writing.

- The use of physical digital storage media such as CDs and USBs in school requires a teacher's permission.
- Teachers or a member of management reserve the right to examine data and materials present on a school device that has been utilised a student. This includes emails and other communications on school approved platforms. This is to ensure the welfare of students, and the safe and focused usage of digital technologies.
- Under no circumstances should a student change or attempt to change the settings of devices or software programmes installed on the device.
- Computer trolley usage is booked through online booking system in VSWare by teachers/staff only.

Use of Mobile Phones and Personal Devices

The use of mobile phones and personal devices is outlined in the school's Mobile Phone and Personal Electronic Devices Policy (See Appendix 3). All members of the school community should be aware of this policy and its stipulations.

In addition, students are prohibited using their mobile phone or other personal devices to link to school devices using Bluetooth or any form of wireless/wired connection.

Data Protection

All members of the school community should be careful around the use and distribution of data, especially that of a sensitive nature. The school recognises the seriousness of its data processing obligations and has implemented a set of practices to safeguard personal data. This AUP and the actions of all members of the school community, including visitors, who use Digital Technology for school related activities are governed by the school's Data Protection Policy (see online) and by legislation. The Irish Data Protection Act (2018) and the European General Data Protection Regulation (2016) are the primary legislative sources. As such, they impose statutory responsibilities on the school as well as providing a number of fundamental rights (for students, parents/guardians and staff and others) in relation to personal data (Data Protection Policy 2019, 1.3).

Sanctions

All school rules apply when students use technology to enhance their learning experience or learn online. Violations of this policy and/school rules regarding technology enhanced learning in John the Baptist C.S. may have disciplinary repercussions up to, including but not limited to:

- Suspension of network and computer privileges.

- De-merit recorded on Vsware
- Referral to Year Head.
- Report card (white/green/red)
- Detention.
- Suspension from school and/or school-related activities.
- Expulsion.
- Legal action and/or prosecution.
- John the Baptist C.S. reserves the right to report any illegal activities to the appropriate authorities, such as the Garda.

Queries related to ICT in John the Baptist C.S. may be directed to info@johnthebaptistcs.ie

Students should be aware that the serious infractions of the school's AUP may result in the suspension and removal of accounts and privileges. This may affect student subject choice, especially at Leaving Certificate as the use of Digital Technology is integral to particular subjects' curricula.

Users should report any suspected abuse of computer and network resources, or any unpleasant material or email that may come to their attention as well as any suspected damage or problems with files to the Principal. When requested, users are expected to cooperate with system administrators and/or other authorised staff in any investigation of system abuse. The school management reserves the right to examine any files held on its computer systems.

Teacher Usage Guidelines

All staff members are asked to be mindful of their Digital Technologies usage policy. The following guidelines and information are in the Teacher Diary available on OneNote. All staff are asked to read and be aware of The Teaching Council's "Guidance for Registered Teachers About the Use of Social Media and Electronic Communication" published in February 2021 (See Appendix 2).

All electronic communication will be issued through the school email system and/or Teams. All staff members are issued with personal, unique school email accounts, passwords, usernames and computer login details. Such accounts should be checked on a regular basis. Use of the Digital Technology is in accordance with these guidelines (Accepted Usage Policy available online) and aims to ensure that students benefit from learning opportunities offered by the school's internet resources in a safe and effective manner.

Data projectors are available in all rooms. Interactive whiteboards are available in Room 15 and Room 25. Please refer to guidelines posted in such rooms for usage of the interactive whiteboards. Prior booking of

the Digital facilities/resources may be made by using VSWare. Teachers are reminded that a video explaining this process is saved on the Whole School OneDrive. Trolleys of laptops are available in each pod and are the property of the school and must be treated with the utmost respect and care at all times. Trolleys must be booked in advance. Any damage must be reported immediately online through VSWare. The Wi-Fi code is available from P. Stack.

Under no circumstances should students have access to the Wi-Fi code.

Guidelines for Computer Rooms

The close of monitoring of students and their behaviour is vital in the computer room. Teachers are asked to explicitly draw attention to the rules of the computer room before the commencement of the first lesson.

- Students are not allowed in a computer room without the presence of a teacher.
- Teachers may assign specific places in the computer rooms for the academic year. Such positions should be noted in the seating template available, copied and placed on the notice board in the computer room. Approved school email accounts are issued to each student in each class, in conjunction with individual, unique passwords and usernames.
Such data should not be shared between students as per the A.U.P.
- No food or drink are allowed in the computer rooms
- Teachers will closely supervise students' use of computers and the internet at all times. Teachers will ensure that students' Internet use will be planned, task-orientated and educational within a regulated and managed environment. Students should use the Internet for educational purposes only.
- Any fault or damage must be entered in the logbook in the room, which is regularly checked.
- Computer rooms and I.T. equipment must be treated with the utmost respect and care.
Any damage must be reported immediately at the beginning of class to the teacher.
- The use of digital storage media such as USB keys or external hard drives requires the permission of a teacher and must be virus checked before accessing in class. Electronic equipment not needed for class is not permitted. Connection to cloud-based storage must be to a reputable source, with the permission of the class teacher and in line with the A.U.P.
- All teachers should make students aware of the A.U.P. The use of social networking sites in school is prohibited. The posting, sharing, commenting on or "Liking" of unsuitable, abusive or disrespectful material is unacceptable. Failure to comply with the A.U.P. will result in withdrawal of privileges, sanctions and may lead to suspension and expulsion.
- Teachers should not remove any ICT equipment from its designated room. Any equipment that is broken or not working correctly should be noted online through VSWare. Doors must be locked when leaving the computer room. Computers must be logged off at the end of each class, logged off and shut down at the end of each day.

Guest Usage Guidelines

The school reserves to right to provide access to the guest WIFI network as needed to visitors to the school. This can be requested from members of the digital learning team. Please note that the password will only be given at the discretion of management or the organising teacher and must not be shared.

Review

This Policy is updated every year or when issues arise.

Signed:

Chairperson

Principal

Board of Management

Date: _____

Date: _____

Date of next review: November 2026

Appendix



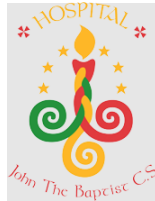
Appendix 1: Draft Guidelines for Registered Teachers about the Use of Social Media

Guidance for Registered Teachers

About the Use of Social Media and Electronic Communication



Appendix 2: Mobile Phone and Personal Electronic Devices Policy



Mobile Phone and Personal Electronic Devices Policy.

Under review

1. Introduction

John the Baptist Community School is committed to providing a safe environment where learning can take place. John the Baptist Community School's mobile phone policy is in keeping with the Mission statement:

Mission Statement

John the Baptist Community School is committed to the provision of a broadly based education in an atmosphere of mutual trust and respect, balancing vision with realism which facilitates personal growth and development among students, staff and community.

2. Scope of this Policy:

This policy covers all Personal Electronic devices (P.E.D.s) which includes:

- Mobile phones/smart phones/smart watches
- All electronic devices including MP3/4, personal music devices, tablets or any other device capable of recording or sending messages. Please note this list is not exhaustive.

3. Rationale

In keeping with our mission statement, the following policy is founded on maintaining a safe, nurturing environment where the personal dignity and rights of the school community are preserved, and the school reputation is safeguarded. The school supports the use of new technology but will not tolerate any abuse of such technology. It is important for students to develop their socialisation and communication skills with peers and over-use of mobile phones impedes this. It must be acknowledged that students need to learn to manage and use devices in an effective manner. The misuse of a personal electronic device could constitute a breach of safety and security for all the members of the school community, as well as having the potential to cause anxiety for recipients of relayed conversations or messages. In this way, it acts as a protection for parents/guardians.

This policy aims to ensure that:

- Classes are not interrupted by P.E.D.s

- Students are concentrating and engaging in class on active learning
- Text/video bullying/intimation/cyber bullying are prevented
- Individual privacy and personal safety are upheld in the school community

Contact with home during the school day

All calls from students to parents/guardians e.g. in event of illness or accident, must be made from the school office, with prior permission sought. This is to ensure that students who may be unwell or ill are fully monitored and cared for as they await collection. Parents/guardians who need to contact students during the day must do so through the school office at (061) 383283. We ask parents/guardians to cooperate and support this policy by not contacting students by mobile phone during the school day.

4. Policy

It is illegal to display or circulate images of another person without their permission. Irresponsible use of camera phones can lead to people's rights being violated. The potential for misuse of these phones in dressing room areas and classrooms exists and, with access to social network sites so readily available, it could have bullying implications. Mobile phones are expensive and the school cannot accept responsibility for loss of, theft or damage to, mobile phones etc. while on school property (this includes confiscated items).

5. If students insist on bringing a mobile phone or other electronic devices to school:

- They must be locked in his/her locker, switched off and not carried on his/her person or in school bags. Parents/guardians may arrange to contact students through the office.
- It is strongly advised that students marked their mobile phones/digital devices with their names and use passwords to insure that unauthorised phone calls cannot be made on their phones. Each student is responsible for all communication from their phone and for any image or recording on their phone.
- The school can accept no responsibility for mobile phones/devices. Devices are brought to school entirely at the owner's risk. The school accepts no responsibility for lost, stolen or damaged devices.
- They must remain switched off during school-based activities. These include games, religious services, concerts and all other school-based and out of school activities.
- As per legislation, audio or visual recordings are not allowed and strictly forbidden. Serious sanctions, up to and including reporting to an Garda Siochana, will apply in the event of unauthorised photographs or recordings.
- The Department of Education & Science does not recognise mobile phones as appropriate for use as calculators or clocks and as such, mobile phones should not be produced by students using this as a pretext.
- In exceptional circumstances (e.g. school trips, out of school matches, foreign trips, out of school hour trips etc.), prior permission may be granted by the school Principal for the use of the mobile phones on request by staff member responsible for the activity. This allows students to contact teachers or parents as necessary. Students participating in school related activities must abide by the relevant rules. Inappropriate use of phones during school related activities is strictly forbidden and sanctions will apply.
- It is the responsibility of each teacher to implement this policy.

6. Sanctions:

- a. Devices being carried by students will be confiscated and held until the end of the day.
- b. Devices being used by students will be confiscated and may be held for one week.
- c. Refusal by students to cooperate in handing over the device will result in the device being confiscated and may held for two weeks.

- d. The teacher will store the device in a designated location in the Deputy Principal's office. They will place them in an envelope and record the name of the student, the name of the teacher confiscating the device and the date of confiscation.
- e. The device may be collected, by students, from the Deputy Principal's office at the end of the day, week or two weeks, as applicable.
- f. Repeated breaches by the same student may result in the device being confiscated and kept for an extended period to allow consultation with parents/guardians as to how best to prevent future breaches. In this case, a parent/guardian must collect the device from the school.

Review

This Policy is updated every two years or when issues arise. Reviewed by: Assistant Principals Don MacGabhann, Mary Sheehan and Rachel Hayes, Parent: Mr Danny Wade, Members of the Student Council in May 2016. Ratified by B.O.M.

Signed:

Chairperson

Principal

Board of Management

Date: _____

Date: _____

Date of next review:



Code of Behaviour

Reviewed by:

- Assistant Principals
- Parents Association
- Teachers
- Student Council Members

Ratified by the B.O.M on: 15th January 2024

Review Date: January 2026

Appendix 3: Digital Learning Insert in Student Journal 2024-2025



The school uses the Microsoft 365 learning platform which contains the following apps to help students on their learning journey;

- **Outlook**--is your email app.



- **Teams**--is where you engage with class work and your teacher.



- **OneNote**—is your digital copybook

These apps should be downloaded to your mobile phone or device at home.

Logging into the Microsoft 365 Learning Platform;

Log on to office.com with your school email.

Your school email is the year you entered the school plus the first letter of your Christian name and your full surname e.g. Jane Doe who starts First Year in September 2024 = 24jdoe@johnthebaptistcs.ie

Creating your password; think security – no names, add symbols, numbers, capitals etc. One helpful approach is to think of a phrase and change /replace letters with symbols e.g. Limerickforliam – L1mEr!ck4Li@m. - Once you have your password set, keep it safe, secure and private – it is only for you. Write it somewhere only you know, not using the word “password”. –

If you lose your password, call into the main office or contact the Digital Learning team – Mr. Stack, Mr. O’Connor or Ms O Donnell - Please follow all instructions and guidelines from teachers and staff regarding device use. –

Digital school bag ;



The digital school bag on the school website has lots of videos and tips to help you. Let the Digital Learning Team know if there is something that needs to be added to these resources. - Self-directed learning is key – digital resources offer a great chance for you to delve deeper into topics and forge ahead in your understanding. Also, our learning platform offers excellent opportunities to collaborate/ work together with other students – make the most of every learning opportunity.

Technology Enhanced Learning Digital learning is an important part of life at John the Baptist Community School and is vital to enhance and develop your learning.