



Technology Enhanced Learning Acceptable Usage of Digital Technologies & Internet Policy 2020/21

John the Baptist Community School

Rationale for ICT 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 ICT and internet 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 If the school AUP is not adhered to, this privilege will be withdrawn, and appropriate sanctions will be imposed.

It is envisaged that school and parent 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 ICT 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 ensure, that at the end of the Senior Cycle, students have acquired key skills and a solid foundation of ICT 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 will take place with an acknowledgment that each group's role is varied and significant.

Students

- Use ICT to open up new forms of learning and collaboration to support different styles of learning.
- Experience joy, satisfaction, passion and success in their education and lifelong learning.

- Actively engaged in learning – both in and out of school.
- Accepting ownership of their learning – involving the ability to be self-directed, a decision maker and a manager of priorities in and out of school.
- Using technology to achieve personal learning goals and to succeed in various learning activities.
- Using ICT critically, ethically and responsibly.

Teachers/Staff

- Taking a more facilitative role, providing student-centred guidance and feedback, and engaging more frequently in exploratory and team-building 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”
- Supporting students to create and innovate so that they are engaged in managing their own learning goals and activities.
- Accepting ownership of their own professional learning and, where appropriate, designing and participating in learning communities that make extensive use of technology.

School Leaders

- Taking 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 (ref) 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.
- Disrespectful behaviour and inappropriate language is not acceptable in any format (written/spoken/pictorial etc.) and in any forum (Teams/OneNote/external apps such as whiteboard/jamboard/mentimeter etc. – this list is not exhaustive). As per the school's Code of Behaviour, all users are expected to act in a manner that is courteous and respectful. The use of inappropriate, unacceptable language affects all students negatively and shows disrespect for other students, the staff, class activities and the school rules. The use of foul language or images distracts from learning and teaching and impacts negatively on the mutual trust between teacher and students, and its use will result in sanctions.
- 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).
- 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 offers allow 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, collaborative commentary on apps and all conversational channels etc. 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 (9th of 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 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. Please note that in the academic year 2019/20, this grace period has been extended to one year to allow for those sitting November exams and to address possible questions concerning calculated grades.
- 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 through email approximately 1 month before finishing school as well as twice more (1 month and 1 week) before the termination of their account.

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, cat-fishing, 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 ICT privileges.
- In some cases, cyber-bullying is a crime and may be reported to the Garda.
- 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, TicToc 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.

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 primary 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.

Sexting & Intimate images

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.

Users should note that The Harassment, Harmful Communications and Related Offences Bill (also known as 'Coco' Law) introduced two new offences to deal with the non-consensual distribution of intimate images. This means it is illegal to distribute or publish intimate images without consent and with intent to cause harm and can result in an unlimited fine and/or 7 years imprisonment. Under the Bill, the second offence deals with the taking, distribution or publication of intimate images without consent, even if there is no specific intent to cause harm. This offence carries up to a maximum penalty of a €5,000 fine and/or 12 months imprisonment.

While offering varied entertainment opportunities, social media is not a suitable forum for school activities and communication or a primary conduit for learning and teaching. The school employs the use of a secure school website and an official school Twitter account. These are administered by limited dedicated individuals within the school and used for promotion, information and display purposes only. The website and Twitter account will be regularly checked to ensure that there is no content that compromises the safety or personal data of pupils 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.

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

Users must not send anonymous email as only a school account should be used for school communication. Neither may they use the email address of another user to send email. 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 the use of images or information to set up a fraudulent account on any form of social media, pretending to be a member of a school community. 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 one 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 those involved 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, with no access to the named owner of the account. An investigation will then occur which may include some or all of the following: 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 the student can work with other students to ensure they do not fall behind.

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, especially the recording of material.
- 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.
- Food and drink are forbidden in all computer rooms as well as classrooms where digital technologies are being used. Students should 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 booked.
- 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 Digital technologies 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 use their own account only. This account should be used for educational purposes only.

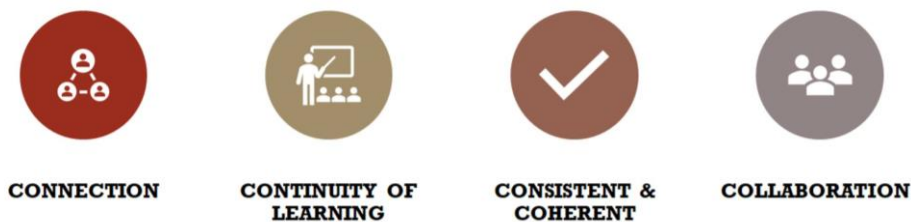
- Students will be provided with training on how to log in to their Office account and how to send emails appropriately with the correct etiquette.
- Uploading/downloading and installation of non-approved software will not be permitted. All relevant requests must be made to the ICT coordinator in writing.
- The use of physical digital storage media such as CDs and USBs in school requires a teacher's permission.
- Any stage, a teacher or member of management reserves 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.
- Students should under no circumstances 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.

Remote/ Blended Learning

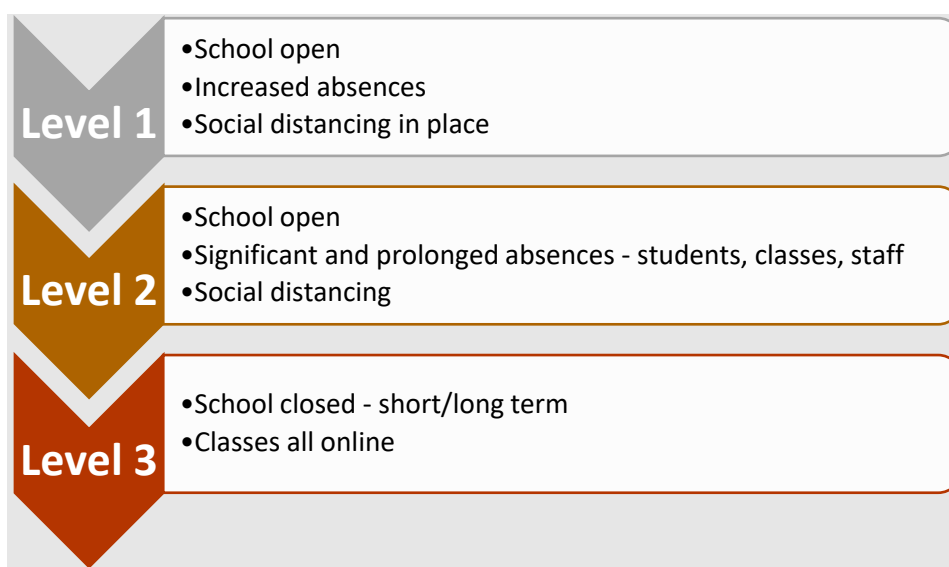
Developments in IT provide great opportunities as learners and teachers. Advances in technology mean that assignments can be delivered remotely and that greater access to information on the internet affords the opportunities for real learning to take place under the watchful and professional guidance of the teacher. A remote teaching period is any time during which the primary means of educational delivery is through online means, as ordered or necessitated by Public Health Guidelines, the Office of Emergency Planning, Governmental/Department of Education directives or those from other such relevant bodies. This can vary in length. **However, whether a child is being directed remotely or via a traditional classroom environment, it is very important that all partners are aware that once a learning exchange takes place between a student and teacher, whether at home or school, the same statutory rules apply i.e. the school's Code of Behaviour and all of the school's policies still apply.**

The onset of Covid 19 has necessitated this move to a blended learning or remote learning model. Please note that John the Baptist Community School has produce a "Continuity of Learning Action Plan" to respond to ever the evolving and changing dynamic surrounding Covid 19 (See Appendix 1) Blended learning is defined as any time a student learns (at least in part) at a supervised bricks-and-mortar location away from home and at least in part through online delivery with some element of student control over time, place, path and/or pace: often used synchronously with hybrid learning (International Association for K- 12 Online Learning 2011: in Barbour 2013).

Core Underpinning Principles of Remote Learning at John the Baptist C.S.



The above four principles underpin all blended, synchronous, asynchronous and distance learning models that may be in play as needed during present and future academic years. More details can be found in the Continuity of Learning Action Plan. Blended learning at John the Baptist C.S. responds to three levels/stages:

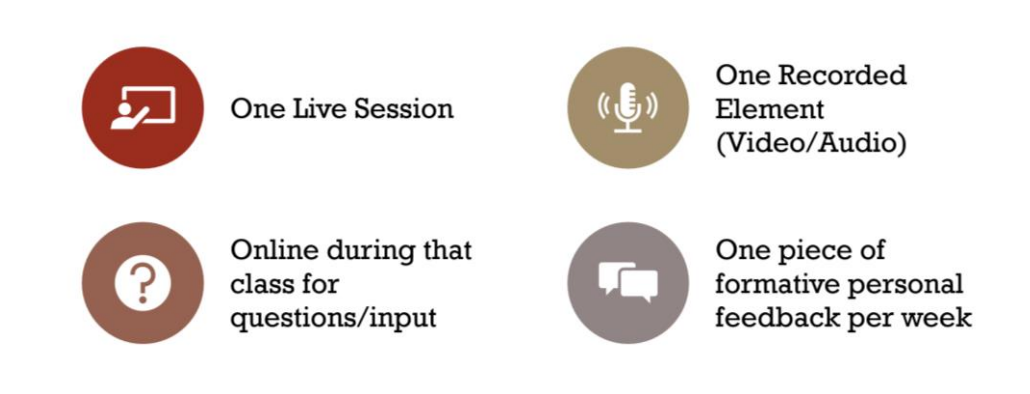


To respond to the school community's needs at that point, a blend of the following will be used (please note this list is not exhaustive):

- Live classes – synchronous learning (full classes, or smaller groups such as for SEN engagement). Please note no recording of live sessions is allowed and would be considered a data breach, resulting in serious sanctions. Any sharing of recording or images taken of a live class/class activities is completely unacceptable and may result in sanctions, up to and including suspension and expulsion.
- Recording classes/instruction – asynchronous learning
- Posted class materials such as presentations, handouts etc.
- Audio recordings and feedback
- Personalised feedback
- Links to suitable external sources, videos and materials
- OneNote postings
- Collaboration activities and opportunities

- Assessment opportunities and formative approaches

During a full remote learning period, all classes will experience the following as a minimum:



Guidance for students on video/live classes

While schools are closed your teachers may provide the opportunity for virtual lessons on Teams. Remember that this is an extension of the classroom and everyone should conduct themselves as they would in a classroom. Participating in video/live lessons is a great way to ensure connectivity with teachers and classmates, but it is important to follow these rules and guidelines.

- Join Teams lessons from an environment that is quiet, safe and free from distractions ideally in a common space and within earshot of parents/guardians (and not a bedroom). A kitchen table, home office or family space is recommended.
- Be on time for your interactive session – aim to be there 5 minutes early.
- Be dressed appropriately for learning in home clothes (e.g. no pyjamas, no vest tops, hats or hoods).
- Remain attentive during sessions and ensure that you are free from distractions. You should not be using personal social media in lesson time.
- You may wish to use headphones to listen to your teacher in online sessions if it helps to avoid distractions.
- Your microphone and camera should be turned off and they should only be turned on if a teacher asked you to do this during the class.
- You are not anonymous. Be mindful of your expressions, language, speaking tones, and what you say. Your voice and video are viewed by everyone participating in the conference. Other people in your house can hear what you and others in the video conference are saying.
- Follow the same classroom rules that you would follow in real life. Listen to the teacher. Take turns to speak. Be kind and considerate. Any use of inappropriate language (words, phrases, emojis etc.) is not acceptable and will result in sanctions. Such inappropriate language is not acceptable in any format (spoken/written/typed/pictorial/audio files etc.) or

in any forum (in OneNote/Teams message/post, collaboration spaces such as Tweetboards or Jamboards or Year Hubs). The use of inappropriate language/comments will result in sanctions, up to and including suspension and expulsion.

- Students must not record or take photos of classmates or teachers during video conferencing sessions, nor share lessons publicly (written or video or sound).
- Think before you speak. Stay on topic. Make sure your comments are clear and appropriate to the conversation. Don't say anything you wouldn't say in your actual classroom.
- Be a good listener. Take the time to listen to what people are saying. Don't interrupt others.
- Think before you type. If your teacher enables the Chat feature you may be able to participate by typing into a chat box. Choose your words carefully. Use appropriate spelling and grammar. Stay on topic. Don't use sarcasm or humour that could be misunderstood. Don't type in all caps.
- Take it slow. Remote learning is probably a new experience for you. Resist the impulse to be silly or to say or type the first thing that comes into your mind.
- Video conferencing/live classes is a privilege. If you cannot use it responsibly your access to school managed video conferencing tools will be removed.
- Students should understand that these rules are designed to help keep them safe online and that if they are not followed, school sanctions will be applied, and parents / guardians contacted. Please see this link to access the school's Code of Behaviour policy.
- Communicate and behave with the same respect and consideration you would use in the classroom
- Classes may be recorded in order to provide additional resources for students and to monitor behaviour
- Complete assignments with integrity and academic honesty, doing your best work
- Do your best to meet timelines, commitments, and due dates. Communicate proactively with your teachers if you cannot meet deadlines or require additional support
- Be mindful of all comments/language/images posted
- Collaborate and support your peers in their learning
- Comply with the school's Acceptable Use Policy, including expectations for online etiquette

Camera Use

The school does not require but advises students to keep their cameras on at all times. This aids student engagement, interest and social interaction. It also demonstrates respect for the teacher, the class and for fellow students. Students are required to have their cameras on for roll call (to ensure identity) and when requested by a teacher for a learning activity e.g. to show a mini whiteboard. Moreover, students are asked to turn on their cameras when in breakout rooms to aid collaboration and connection. Guidance and instructions on using their camera and mic in a live class are available on the school website.

Digital Learning Charter

Please note that all students were asked to read, review and sign the Digital Learning Charter. This is shared with all students through the Year student hubs.

Please see Appendix 5 for the charter.

Do think	Do think before you post. Complete the reading or preparation work before you write.
Do post	Do post your response early to give your classmates more time to reply. Check back later to see what comments have been added.
Do explain	Do explain your opinion and use examples to help others understand your points.
Do post	Do post something that furthers the discussion and shows depth of thought. The best part of a discussion board is that you get lots of think time before you post. Use it.
Do reply	Do reply to several of your classmates' posts, adding examples or asking questions.
Do remember	Do remember that it is harder to tell when something is a joke online. Use humour sparingly.
Don't agree	Don't agree with everything you read. It makes for a really boring conversation. Politely disagree when you have a difference of opinion.
Don't reply	Don't reply to the same people each time. Try to bring in other voices.
Don't get	Don't get personal. Focus your criticism on ideas and arguments, not on your classmates
Don't bring	Don't bring the outside in. No inside jokes, references to people who aren't in the conversation, or comments you wouldn't say face-to-face.

The following diagram has been developed by the Digital Learning Team to guide students as to expectations during a live class:



Any student who does not adhere to the expectations and guidelines above may be subject to sanctions.

Students are also asked to:

- Engage fully with all asynchronous recordings/materials that may be posted
- Post/return work as needed through the method outlined by their class teacher (e.g. assignments, OneNote)
- Check their calendar regularly for updated and events
- Check their email (Outlook) daily for notifications
- Respond if contacted by their teacher
- Notify their teacher/member of the Digital learning team if they are having any technical issues.

Guidelines for Parents/Guardians supporting Distance Learning

Distance learning may be challenging for families. Parents may need to think differently about how to support their children, how to create structures and routines that allow their children to be successful, and how to monitor and support their children's learning. Some students will thrive with distance learning, while others may struggle. The guidelines provided below are intended to help parents think about what they can do to help their children find success in a distance learning environment. Please see the diagram developed by the DLT to help:

John the Baptist Community School Office 365 Education

GUIDE TO Microsoft 365 FOR PARENTS & GUARDIANS

WHAT DEVICES DO STUDENTS NEED ACCESS TO?

Must Have... Smart Phone, Tablet, Laptop / PC

Not required but can help...

WHAT APPS SHOULD STUDENTS HAVE DOWNLOADED?

- Teams**: Communication tool for learning intentions and resources
- OneNote**: Digital Notebook for organising notes, using a range of digital media
- Outlook**: Student email for one on one communication
- OneDrive**: Online cloud storage for student files

HOME LEARNING

WHERE DO STUDENTS ACCESS HOMEWORK ONLINE?

- Instructions are often posted on Teams. Files and other learning materials may be found through Teams or OneNote

HOW DO STUDENTS SUBMIT HOMEWORK ONLINE?

Hand Written

- Written work is photographed and uploaded to Teams or OneNote depending on the task

Digital Files

- Students have access to Word, PowerPoint and Excel which can all be edited on their smart phone

HOW CAN STUDENTS ASK QUESTIONS ONLINE?

- Teams allows students to ask questions in a forum that can be answered by their classmates
- Teachers can be emailed however do not expect replies after 3.40 pm

See the digital schoolbag on the homepage of the school website for videos on how to upload work to Teams and OneNote

TROUBLESHOOTING

ISSUES LOGGING IN

1. Make sure address is www.office.com
2. Ensure email address is typed correctly: @johnthebaptists.ie
3. Ensure caps and numbers are entered as given for the password

LOST PASSWORD

Email info@johnthebaptists.ie

CLASSNOTEBOOK WONT APPEAR IN ONENOTE APP

1. Go to www.office.com on a web browser and log in using your school account
2. Go to the OneNote App
3. Go to the Class Notebook Tab
4. Select and open the Notebook that is not appearing in the app
5. Go back to the app and select more notebooks
6. The notebook should appear

HOMEWORK WONT UPLOAD FOR TEACHER FEEDBACK

1. Always swipe down once homework is uploaded to ensure correct syncing
2. If the issue persists, uninstall all school apps
3. Reinstall and log in to the apps in the following order:
 1. Teams
 2. OneNote

WHAT CAN I DO TO HELP MY STUDENT?

- ✓ Stay up to date with work by downloading the school apps to your own phone and logging in with your student's details
- ✓ Check out the digital school bag on the school website for video tutorials
- ✓ Keep a copy of your student's password

[Click here for more info on Microsoft 365 for Parents/ Guardians](#)

General Guidelines

1. Establish routines and expectations. Talk with your student regarding the expectations and guidelines associated with online learning and engagement.
2. Define the physical space for your child's study; it should be a space/location where their children will learn most of the time, be a public/family space, not in a child's bedroom. It should also be a place that can be quiet at times and have a strong wireless internet signal, if possible.
3. Monitor communications from your children's teachers as teachers will communicate with parents through the Year Head, when and as necessary. Please take note of any messages/letters sent by the school to update and inform.
4. Begin and end each day with a check-in. Parents are encouraged to start and finish each day with a simple check-in. In the morning, ask what is your child learning today? What are their learning targets or goals? How will they spend their time? What resources do they require? What support do they need? This helps students to process the instructions they've received from their teachers. It helps them organise themselves and set priorities.
5. Take an active role in helping your children process and own their learning. Human beings learn best when they have opportunities to process their learning with others. In virtual learning platforms that opportunity is limited. Parents should regularly engage with their children about what they're learning to help them to process it. However, it's important that your child own their work; don't complete assignments for them, even when they are struggling.
6. Establish times for quiet and reflection
7. Inform the school if your student will be unable to attend a live class or engage online
8. Encourage physical activity and/or exercise
9. Remain mindful of your child's stress or worry
10. Monitor how much time your child is spending online
11. Keep your children social, but set rules around their social media interactions
12. Talk to your children about safety online and healthy internet practices

Non-engagement by students

During a full remote learning period, engagement by students is vital to ensure the full continuity of learning. Users should be aware that Insights, a specialist app with the Microsoft suite, allowing teachers to monitor all aspects of student engagement is used throughout the school's system. Students who do not engage in live classes, fail to submit some/all of work given or engage with class activities posted by teachers will be first contacted by teachers, offering them the opportunity to re-engage. If a student does not respond, teachers are asked to submit a short report on such non-engagement through a dedicated, secure collection form.

Texts will be sent home for all those who have been reported, When a student has not responded to such intervention, the team may pass that name onto their Year Head, Senior Management/Principal and if deemed necessary, the Guidance Counsellor/Cabhair. The school will also send text messages with key information or reminders to the school community at various times.

Any misbehaviour such as that outlined in this policy may result in sanctions and the use of the schools report system, demerits etc.

Wellbeing during Remote Learning

The increased use of screen and online materials must be balanced with a healthy lifestyle. All students are reminded to take regular exercise, time away from screens (especially prior to sleep), get air and to practice wellbeing activities as suggested by their Religion, Wellbeing, SPHE, CSPE teachers and indeed all the school community. Please see the school website for resources to help in the dedicated page "Keeping well during Covid".

All members of the school community are asked to communicate online only between school hours to ensure a healthy work-life balance

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 those...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 in Journal**
- **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 computer use 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 ICT usage. The following guidelines and information is in the Teacher Diary. 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. 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 internet is in accordance with these guidelines (Accepted Usage Policy available on online/staffroom

computers) 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 ICT facilities 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.

All students asked to wipe down all devices prior to and after use and keep their social distance when retrieving the device from the trolley. Students must use the wipes provided. Sprays cannot be used on devices. Students are also asked to login to the online Laptop Trolley user log (on the front page of the school website). This is to ensure that effective contact tracing concerning devices can be completed.

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 will 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 or indeed “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.

Remote Teaching

All staff should be aware of the Continuity of Learning Action Plan for all three levels.

A synchronous class can take many forms, e.g. Teams live class.

Suggestions/considerations when planning and running a live class on Teams:

1. Keep classes short and within the timetabled slot
2. Login ahead of students and greet them when they enter “class.” All teachers are asked to call a roll during live classes.
3. Set up Chat parameters, e.g. public chatting only when hand up and asked by the teacher, otherwise student microphone is muted.
4. Once class begins, mute students on entry or establish some shared Teams norms, such as: mute your mic when not speaking, say your name before you participate (sometimes it’s hard to tell who is speaking). Teachers are reminded about the use of the lobby and meeting settings
5. Remind students that the same digital technology rules apply to a virtual classroom as to the physical classroom. No taking or posting images/video of classmates and instructors to the web or to Social Media without permission.
6. Begin your instruction by sharing your screen; it may show the outline of the work for the week, point out where the resources and assignments for that week are located. Teachers are reminded to share the 5Ws and 1H of their schedule
7. Preview your objectives for the virtual class and any expectations you have of them during the call (notes, participation, response online after class, etc.)

8. Record the live classes as needed for later reference or for use in revision, or for students to access if they were absent/unwell.

Suggestions/considerations when assigning pre-recorded or independent learning materials:

1. Post as early as possible to allow maximum time for students to engage.
2. Inform students explicitly where work may be found. Tagging the class Team is of benefit here as students receive a notification.
3. A consistent approach works best for point 2 as students are familiar with where to find assigned work i.e. OneNote, Teams etc.

Guest Usage Guidelines

The school reserves the 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 and it must be typed directly into the user's device.

Review

This Policy is updated every year or when issues arise.

Signed:

Chairperson

Principal

Board of Management

Date: _____

Date: _____

Ratified by BOM: 08/03/2021

Date of next review: March 2022 or as necessary

Appendix



Guidance for Registered Teachers

About the Use of Social Media and Electronic Communication



Full document available at <https://www.teachingcouncil.ie/en/publications/fitness-to-teach/guidance-for-registered-teachers-about-the-use-of-social-media-and-electronic-communication.pdf>

Appendix 2: Continuity of Learning Action Plan

John the Baptist Community School

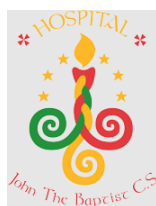
Continuity of Learning Action Plan

for Covid-19



Please see link for full document:

Appendix 3: 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 safe-guarded. 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 mark their mobile phones/digital devices with their names and use passwords to ensure 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 Síochána, 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 be 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:

Review Date: September 2021

Appendix 4: Insert in Student Journal 2020/21

Digital Learning – Technology Enhanced Learning

Digital learning is an important part of life at John the Baptist School and is vital to enhance and develop your learning. The school is a Microsoft 365 learning platform school which means that every student has access to the full suite of Microsoft programmes to help them on their learning journey.

When you login – *Outlook* is where you will find your emails, *Teams* is where you engage with classwork and your teacher.

Some helpful tips:

- Log on to office.com with your school email. Your school email is the year that you started in the school, with the first letter of your Christian name and your surname e.g. 19jdoe@johnthebaptistcs.ie
- When 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. However, it is compulsory that you share you login details and password with your parents/guardians, who are free at any point to login to check your online learning progress.
- If you lose your password, contact the Digital Learning team – Mr. Stack, Mr. O'Connor or Ms. Hayes
- Please follow all instructions and guidelines from teachers and staff regarding device use.
- The digital school bag on the school website has lots of videos and tips to help you. This will continue to grow. Let the Digital Learning Team know if there is something that we need to add 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.
- Remember that you can download the Microsoft apps from iOS or android store – Office, Outlook, Teams etc.

Appendix 5: Digital Learning Charter

Please note the following is shared through the Year Hubs. All students are asked to read and agree to it.

CHARTER

Please read the statements below:

- I am aware that my actions online have a huge impact and must always be respectful and in line with our school rules.
- I understand that my Office 365 account (e.g. apps such as Teams, OneNote, Outlook, OneDrive etc.) is a school account and should not be used for any other activity than school.
- I understand that only school material must be posted, saved and shared using or on my school account/apps and that all such material must be respectful
- I must fully engage in all parts of blended learning in my subjects - live class, recordings, posts, file sharing, assignments etc.
- I have read, understand and agree to all of the expectations of students for live classes
- I understand that I must create a suitable learning space, that is free from distractions such as other people, devices, noise etc. By creating a distraction free learning space, I can learn best, engage fully and be a valuable member of classes.
- I understand that I can access my class materials in lots of ways - on a computer, phone, with gaming systems such as Xbox and Playstation, tablets etc.
- I value my own ability to upskill by using the Digital School Bag on the school website, which has lots of links and videos to help me
- I accept that it is my responsibility to visit my class Teams every day, reviewing all parts of the Team such as the class notebook to make sure I do not miss anything
- I know that my password is very important information and should not be shared with anyone.
- I acknowledge that I must ask teachers questions through Teams if I am unsure of any aspect of online learning.
- I accept that it is my responsibility to submit work in the timescale given and to make sure it uploads fully.
- I understand that I can only contact a teacher during school hours 8:50am-4:00pm and not by email so that we can all have a good balance between school and home.
- I understand that any disrespect shown to staff or another student online in any form will not be tolerated and will result in serious sanctions. This includes the sharing of any material that is inappropriate and/or may cause upset to someone else.
- I will regularly visit my Year Hub to see announcements that are important to all students in my year group.
- I know that if I have any problems, I can contact my class tutor, year head, any member of the guidance team, a deputy principal or principal.

- I understand that I cannot record any live class or content and that anything that needs to be recorded will be done so by my teacher and sent to me. Any recording of a live class or online material by a student is a data breach, will be dealt with seriously and will be reported to the Data Protection commissioner. I am aware that live classes may be recorded by teachers for students' use at a later stage and this will be shown by a red dot in the top left hand corner. I can let my teacher know if I have any issues or questions. These recordings will only be shared with the given class for revision purposes.

- I recognise that I must look after myself, making sure I exercise so I can have a balanced and healthy digital learning experience.

- I will always try to be positive and proactive to make my digital learning experience the very best it can be.