# Acceptable Usage Policy

This Policy applies to all of the school's "Devices", which means all computers, iPads, laptops, smart phones and other IT resources that connect to the school's network.

This Policy applies to staff and students of St John's Parochial NS. The School reserves the right to amend this policy from time to time entirely at its discretion.

This Policy should be read carefully to ensure that the content is accepted and understood The aim of the Acceptable Use Policy ("AUP" or "the Policy") is to ensure that students benefit from the learning opportunities offered by internet access in a safe and positive manner. This Policy also aims to establish minimum standards for, and let the students, parents/guardians know of the school's administration and monitoring of, the schools devices, equipment and networks.

## School

The School employs a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies include, but are not limited to the following:
A firewall is used on school Devices to minimise the risk of exposure to inappropriate material and to block unsuitable sites. This is regularly updated.
• Students and teachers will be provided with training by teachers in the area of research techniques specific to the Internet.
• Online safety training will be provided to teachers and will be taught to all students.
• Uploading and downloading of non-approved software on school Devices will not be permitted.
• Virus protection software is used on school Devices and updated regularly.
• A teacher will always supervise Internet sessions which are conducted on school Devices.
• Websites will be previewed / evaluated by a teacher using a filtering system, before being integrated into lessons conducted on school Devices.

The School's search engine has a built in 'safe search' feature. The 'safe search' feature will be enabled on all search engines on school Devices.

• It is important to note that the school's Anti-Bullying Policy should be read in conjunction with this Policy. Parents/guardians and students should be aware that placing a once-off, offensive or hurtful internet message, image or statement on a social network site or other public forum where that message, image or statement can be viewed and/or repeated by other people will be regarded as bullying behaviour.

## Use of the Internet

• Students will be taught specific lessons on online safety by teachers.

• Students will not knowingly attempt to visit Internet sites on school Devices that contain obscene, illegal, hateful or otherwise objectionable materials and the school will not be responsible for any attempts taken in this regard.

• In the event of accidentally accessing any of the above sites, the student will be expected to immediately turn off the monitor and report the incident to a teacher or supervisor.

• The internet will be used to enhance learning and will be used for educational purposes. All websites used by the teacher will be vetted in advance by the teacher.

• Students will not upload, download or otherwise transmit material that is copyrighted on school Devices.

• Students will not disclose or publicise personal or confidential information to others online. Examples of this are, but not limited to, their own or classmates' home addresses, telephone numbers, email addresses, online profile information or name and location of their school.

• Students will not examine, change or use another person's files, username or passwords.

• Students will be aware that any usage, including distributing or receiving any information, school-related or personal, may be monitored for unusual activity, security, and/or network management reasons.

• The school takes every reasonable precaution to provide for online safety, but it cannot be held responsible if students access unsuitable websites either deliberately or inadvertently.

## Email / Google Drive

• When using Google Classroom and the Gsuite Apps, students will use approved class email accounts under supervision of a teacher or parent/guardian.

• Students will not send or receive any material that is illegal, obscene, defamatory, or that is intended to annoy or intimidate another person.

• Students will not reveal their own or other people's personal details, such as addresses or telephone numbers or pictures.

  • Students will never arrange a face-to-face meeting with someone they only know through emails or the Internet.

• Students will note that sending and receiving email attachments is subject to permission from their teacher.

## Distance Learning

  • In circumstances where teaching cannot be conducted on the school premises, teachers may use Google Classroom, Google Meet, Zoom, SeeSaw, Study Ladder,

Padlet or other platforms approved by the Principal as platforms (the "Online Platforms") to assist with remote teaching where necessary.

- Only whole class or group sessions are allowed. Teachers will not conduct 1:1 video, audio or chat sessions with a student.
- When the live online session is finished, the teacher will wait for all students to exit the meeting before leaving. (This ensures that students do not continue chatting without the teacher present).
- Live recordings of the children will not be permitted
- Most sessions should be no more than 20-30 minutes each.
- The school has signed up to the terms of service of the Online Platforms in use by the school.
- The School has enabled the most up to date security and privacy features which these Online Platforms provide.
- In the case of Google Classroom and Google Meet, parents/guardians must grant access to their child to have a school Gmail address such as pupilname.student@stjohnsns.ie
- Parents/guardians will be provided with the password and will be expected to monitor their child's use of the Gmail address and Online Platforms.
- If teachers are using Zoom, parents/guardians must consent to their child having a school email address as above to allow their child access to the lessons. Where the child does not have a school email address, parents can consent by submitting their own email address for their child to access lessons on Zoom.
- Parents/guardians must also agree to monitor their child's participation in any such lessons conducted on the Online Platforms.

## Teleconferencing

The use of teleconferencing requires students and teachers to observe the following rules in order to ensure that both staff and students benefit from this way of teaching and learning. Students and Staff should never;

- Post, stream or transmit any content, including live video, that violates this Policy in such a way that is offensive to students / staff.
- Do anything illegal, facilitate any illegal activity, or promote violence.
- Do anything that threatens, exploits or otherwise harms children or fellow students.
- Engage in any activity that is harmful, obscene, or indecent. This includes offensive gestures, displays of nudity, violence, pornography, sexually explicit material, or criminal activity.
- Engage in any activity that is fraudulent, false, or misleading.
- Engage in any activity that is defamatory, harassing, threatening or abusive.
- Store or transmit any data or material that is fraudulent, unlawful, harassing, libelous, threatening, obscene, indecent or otherwise inappropriate.
- Send unauthorized messages or irrelevant material.
- Misrepresent a user's identity or affiliation with any entity or organization, or impersonate any other person.
- Harvest, collect, or gather user data without consent.
- Violate or infringe any intellectual property or proprietary rights of others, including copyrights.

- Violate the privacy of others or distribute confidential or personal information of others

## Setting up the technology and environment
- Provide clear instructions to students on how they can access the video lesson and if there are passwords needed to access the online classroom.
- Pre-set your video lesson to mute participants' microphone automatically upon entry. You can choose to switch them on selectively to allow student participation.
- It's important to start with the teachers camera turned on. This reinforces to students this is a live session, and establishes a more personal connection with students. However, after a short while, the camera can be turned off to preserve bandwidth and focus students on learning.
- Where possible students and teachers should be in a quiet space with a simple background behind them. The background where possible should not include thoroughfares or active spaces that might accidently lead to inappropriate vison or distractions.

## Preparing for a video conference class
- Prepare an agenda or plan for each class that you can share at the beginning. This gives students a clear idea of how the class will progress, what will be covered, and the activities they'll engage in.

## Running a video conference classroom
- The video conference room is a classroom and the same school behaviour and discipline policies apply to this environment.
- Do not allow any unauthorised access to the video conference room.
- All invited guest adult speakers must be Garda Vetted by St John's Parochial NS in advance.
- Remove any uninvited participants if needed, if you are the host.
- Add a password to the room to ensure extra security when using Zoom.
- A teacher should enter the room before the start time. Students should not be in the online room without a teacher who is the host or co-host for the lesson.
- Turn off student cameras unless they need to demonstrate their learning to the class. In most programs individual camera access can be enabled and disabled as required by the host.
- Limit students' ability to chat amongst one another during a lesson unless it is required for group work. An in-meeting chat can be disabled by most software for the entire lesson.

## Guidelines to Support Schools using Live Video with Students
- Discuss online behaviour and expectations of the students in your first virtual class.
- Give clear and explicit instruction for the technology so they feel supported and regularly clarify their understanding.
- Embrace the pause. Take a moment after the end of your comments and allow for students to ask questions and engage before continuing on.
- Take time to promote questions, comments, and interactions from your class. Allow time for your students to raise their hand, write their questions in chat, or be unmuted to ask their questions live.
- When a student turns on video acknowledge them and any features of their background that may be visible. This allows the teacher to raise awareness that the environment of the student is visible to all the class.

- Speak slowly and clearly.
- You have to bring the energy into the classroom even when there is a perceived lack of engagement/response from the students.
- As the students become more confident in the online space, perhaps allow them to lead discussions or conversations. As in a physical classroom, the teacher doesn't need to run all the activities but do ensure that they the expectations are clear and all students know what their role is.
- Have students be the presenter and share projects with the class. This allows your students to show what they're working on while practicing their presentation skills. It also allows students to hear from one another.
- Try to make the lessons interactive and engaging by varying the way you deliver the lessons. Use the live lesson as an opportunity to collaborate, discuss and brain storm ideas.
- Try to inject some wonder and fun into your online lesson. This is a time for the students and teacher to meet up and establish a social connection. Try a wonder of the week, fun facts or topic related puns.
- As you get more confident with using the tools experiment with some more advanced features such as white boarding tools, annotation tools, polls, screen sharing and breakout sessions to add variety to the lessons.
- Restrict the length of a video lesson to 20-30 mins to maintain student focus.

### For Pupils
- Find a comfortable, quiet space at home where you can work effectively (i.e study desk or table in family room)
- If invited to join a video-conferencing call, pupils must be suitably dressed (not in pyjamas)
- Complete learning tasks with integrity, always doing their best
- Any child who cannot take part in a live video conference can tune into recorded sessions. However any conference where pupils are visible and/or audible will not be recorded.
- Students cannot record or snapshot any element/s of an online or recorded lesson and/or post to Facebook or other online platform

## Internet Chat

• Discussion forums on will only be used for educational purposes and will always be supervised.
•Students will never arrange a face-to-face meeting with someone they only know through emails or the Internet and this is forbidden

## School Social Media sites.

- The School's Facebook account is St John's Parochial School, Co. Kerry.
- The School's website is http://stjohnsschooltralee.weebly.com/
- Students will be given the opportunity to have photos, projects, artwork and other work relating to curricular and extra-curricular school activities published on the school's social media accounts as per the consent form. Teachers will coordinate the

publication of this material.

• Personal information relating to the student including their name, home address and contact details will not be included on school social media or the school's website.

• Digital photographs and audio or video clips of individual students will not be published on affiliated pages, without prior parental/guardian permission as per enrolment form. Instead, photographs etc. will focus on group activities, where children will not be named.

• Photos/Videos may be used for the production of the Homework Journal or specific school events e.g. Communion etc. These photos/videos and the photos/videos on our website/App should not be copied or posted to any social media or other website or published in any way.

• Parent(s)/guardian(s) are requested not to 'tag' photographs or any other content which would identify any children or staff in the school.

• Parent(s)/guardian(s) are requested to ensure that online messages and/or comments to the school's social media sites are respectful. Any messages written on social media are treated in the same way as written messages to the school.

- The Principal will review the content of the website and the social media sites regularly. The Principal and the Board welcome any suggestions about how the content may be improved.
- If any parent or guardian has any concern about the appropriateness of the content of the website or social media sites, then the Board asks that the matter be brought to the attention of the Principal as a matter of urgency.
- This Policy should be read in conjunction with our Data Protection Policy.

## Personal Devices

• Students may not use any personal device with recording or image taking capability while in school or on a school outing. Any such breach of the Acceptable Use Policy (AUP) will be sanctioned accordingly.

• Any images or recordings taken by class teachers on smartphones or other personal devices must be downloaded onto the school server and/or on to the school App/relevant school affiliated website and then immediately deleted from source.

• The use of E-readers may be permitted, under the supervision of the teacher.

All personal devices are to be turned off during school hours.

## Legislation and Regulation

The school will provide information on the following legislation relating to use of the Internet with which teachers, students and parents/guardians should familiarise themselves where appropriate:

• EU General Data Protection Regulations 2018
• Anti-Bullying Guidelines for Primary Schools 2013
• Data Protection (Amendment) Act 2003
• Child Trafficking and Pornography Act 1998
• Video Recording Act 1989
• The Data Protection Act 1988
• Interception Act 1963

## Support structures and Education

• The school will inform students and parents/guardians of key support structures and organisations that deal with illegal material or harmful use of the Internet.
• On an annual basis, the school will run a programme on acceptable internet usage, for students and parents/guardians. This will cover several topics including cyber-bullying.
• Staff will regularly partake in Continuous Professional Development in relation to the development of AUPs, internet safety and cyber-bullying.

## Use of Information Communication Technology ("ICT") Resources

St John's Parochial NS information and technology resources (e.g. e-mail, computers, computer applications, networks, internet, intranet, facsimile, phone and other wireless communications devices, telephone, paging and voice mail systems and the like) are school property and are provided solely for school related activities.

Inappropriate use including hacking, pirating software, using school resources for non-school commercial activities, soliciting, distributing literature for outside entities, disclosing confidential information of the school, sending inappropriate e-mail or accessing inappropriate web sites (such as those advocating hate or violence, containing sexually

explicit material promoting illegal activities), or using school resources in a way that violates the letter or spirit of the school's policies or reflects negatively on the school is forbidden.

Users of the school's information and technology resources must not share passwords. If you allow others to use your password or assigned resource, you will be held responsible for their use.

Consistent with national laws, the Board of Management reserves the right to monitor the use of its information and technology resources and to take appropriate disciplinary actions, or denying future access privileges in cases of misuse. Staff/student use of the school's information and technology resources constitutes consent to such monitoring. All such monitoring will be conducted in accordance with law including, where applicable, the EU's General Data Protection Regulation ("GDPR").

## Sanctions

Misuse of the Internet or any activity which is in contravention with this Policy, may result in disciplinary action, including written warnings, withdrawal of access privileges, and, where appropriate, suspension or expulsion in line with the Code of Behaviour.

The school also reserves the right to report any illegal activities to the appropriate authorities. Access to the Internet will be withdrawn from students who fail to maintain acceptable standards of use.

Signed:
Principal: _Mike O'Toole_ Date: _22-10-'20_

Chairperson: _Jim Stephens_ Date: _22/10/20_

Dear Parent(s)/Guardian(s),

The staff and Board of Management of St John's Parochial School have recently reviewed the school's Acceptable Use Policy (A.U.P). Please familiarise yourself with this policy, prior to completing the A.U.P Permission Slip. School files will be updated accordingly and this form will be kept on file for no longer than is necessary.

## Acceptable Use Policy Permission Slip

Name of student: _____

Class/Year: _____

Parent/Guardian,

As the parent or legal guardian of the above student, I have read the Acceptable Use Policy and grant permission for my child to access the Internet. I understand that students may not be able to participate fully in lessons involving PCs, laptops, iPads and other IT equipment without consenting to our Acceptable Use Policy.

Parent/Guardian Signature:_____