ST. JAMES' SCHOOL
CAPPAGH

PRO PACE LABORA

St James'N.S.

AUP (Acceptable Use Policy)

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

This Policy applies to staff and students of St. James' NS ("the School"). 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 every 2/3 years in the school.
- 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 Aladdin, GSuite/ Google for Education, SeeSaw, Kahoot, Mentimeter Padlet, Zoom, Webex or other platforms approved by the Principal as platforms (the "Online Platforms") to assist with remote teaching where necessary.
- 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 Seesaw, parents/guardians must grant permission for their child to have a school account.
- Parents/guardians will be provided with the password and will be expected to monitor their child's use of the Online Platforms.
- Google Meet, Zoom, Webex or any other form of online live video call will only be used when necessary and with caution. If teachers are using a live video method of communication then parents/guardians must consent to this by submitting their own email address for their child to access lessons in this way.
- Parents/guardians must also agree to monitor their child's participation in any such lessons conducted on the Online Platforms. Parents/Guardians must agree to ensure their child's behaviour adheres to the St. James' NS Anti-Bullying Policy, Code of Behaviour, Acceptable Use of Technology and other relevant policies.
- Parents/Guardians, children and staff must not use devices to record and/or alter in any way audio, image or video – live or pre-recorded - unless specifically permitted by the school.
- Parents/Guardians, children and staff must also be vigilant in terms of child protection with regards to recording children online.
- Parents/Guardians, children and staff must ensure that they never share any media of children in school online, including their own social media profiles unless expressly permitted by the school and anyone appearing in the media.
- Emails sent by and to staff members should be respectful in tone. A staff member is entitled not to respond to an email that they, themselves, deem to be disrespectful in tone. It is recommended that a staff member who receives an email like this makes contact with the principal and agrees a suitable means of communication with sender.
- Excessive contact from an individual, staff to parent, parent to staff, staff to staff is unacceptable. Parents and staff have the right to ask for less communication.
- Any form of email or online communication that falls under the definition of harassment will be treated in the same manner as any other form of harassment.
- Avoid any negative conversations about children, staff or parents/guardians on social media and messaging (Whatsapp, Messenger etc.) accounts. If you have an issue with something in the

school, social media and messaging apps are not the place to raise it. When inappropriate communications are reported, the School will request they are deleted.

Internet Chat

• Discussion forums on Google Classroom 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 Website and affiliated Social Media sites, School App.

- The school's website address is: www.cappaghns.com
- The School uses the Aladdin Connect App as a communication method.
- 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 website as per the consent form. Teachers will coordinate the publication of this material.
- Personal information relating to the student including their full name, home address and contact details will not be included on school social media or the school's website. First names are to be used only.
- Digital photographs and audio or video clips of individual students will not be published on the school website and/or affiliated pages, without prior parental/guardian permission. 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 relating to the school are respectful. Any messages sent digitally or written on various platforms are treated in the same way as written messages to the school.
- The Principal will review the content of the website 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.

Web 2.0

With the advent of Web 2.0, the Internet has become a two way communication system for the school and the wider community. Services such as Aladdin, Seesaw, Class Dojo, gmail and other platforms are being used by the school to communicate with parents and also for parents to communicate with the school. These services, although not owned by St. James' NS, form part of our web services and all content that is placed on these services falls under this policy

The safety of our children on the web is of utmost importance so the following rules apply to the school and parents. Web 2.0 is open to potential dangers when used inappropriately. We would ask:

- Many social media sites have minimum age requirements. While the school will not monitor this, we would advise parents to not allow their children to have personal accounts on Facebook, Twitter, etc. until they are the appropriate age.

- Parents and guardians are encouraged to regularly check their child's online activity / digital footprint. Parents are encouraged to check social media apps (e.g. Facebook, Snapchat, Viber, Whatsapp, Instagram etc) on mobile phones and electronic devices to ensure they are aware of their child's online interaction with others and approve of same.

- Please do not "tag" photographs or any other content which would identify any children or staff in the school.

- If you are uploading a photograph, please ensure that it does not identify the child in any way. Please make sure photograph size is kept as small as possible (no bigger than 800x600 pixels)

- Avoid any negative conversations about children, staff or parents on social media accounts

- Please do not request to "friend" a member of staff in the school. The staff would like to keep their personal lives personal. It may be awkward for a staff member to be asked to ignore a Facebook or other social network request.

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.
- Personal devices should only be in school under exceptional circumstances and prior permission must be sought from the class teacher/ school principal. All personal devices must be turned off during school hours. If a child is required to bring a mobile phone to school to make contact with their parents after school, the mobile phone should be left in the office for the duration of the school day.
- Children are not allowed bring personal devices on school tours or to other out of school events.

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 a biennial 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. James' National School's 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").

Cyberbullying

Bullying is repeated aggression, verbal, psychological or physical conduct by an individual or group against others. Bullying is always wrong and is unacceptable behaviour which should never be overlooked or ignored.

Cyberbullying refers to bullying which is carried out using the internet, mobile phone or other technological devices. Cyberbullying generally takes a psychological rather than physical form but is often part of a wider pattern of 'traditional' bullying. It can take the form of sending nasty, mean or threatening messages, emails, photos or video clips, silent phone calls, putting up nasty posts or pictures on a message board, website or chat room, saying hurtful things in a chat room, pretending to be someone else in a chat room or message board or text message and saying hurtful things, or accessing someone's accounts to make trouble for them

- Any form of harassment using electronic devices, commonly known as cyberbullying is prohibited and will not be tolerated.

- Students are encouraged to report an incident or any communication that constitutes cyberbullying to the school or any member of staff.

- The school will take any report of cyberbullying seriously and will investigate credible reports immediately.

- Students who make a report are requested to preserve evidence of cyberbullying, e.g. a screenshot or a copy of an email, text message, picture or any other electronic form.

- Staff will take appropriate action and will bring it to the attention of the principal when students report an incident of cyberbullying.

- Staff will attempt to preserve evidence of the cyberbullying and will submit any evidence to the principal.

- Bullying will not be tolerated and parents will be expected to co-operate with the school at all times in dealing with instances of bullying in accordance with the school's Anti-Bullying Policy.

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.

REVIEW:

Timeframe for Review: _______________

Responsibility for Review:__________________

RATIFICATION AND COMMUNICATION:

Ratified by Board of Management on __________________
Date

Signed ____
Chairperson, Board of Management

Appendix 1

Dear Parent(s)/Guardian(s),

The staff and Board of Management of St. James' NS 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: _________________________ Date: __________________

School Website and Other publications (e.g. Green & White, Local / National Newspapers)

I understand that my child's schoolwork/photo/video may be chosen for inclusion on our school's website and/or affiliated school pages. In principle, children will only be pictured in groups and will be not be named in full (If full name is given then no image ; If image is given then forename only) (unless prior consent has been given).

Please tick the appropriate box(es) and sign to confirm that you accept;

☐ Use of child's photo/video/schoolwork on School App, Newsletter and school website.

☐ Use of child's photo/video/schoolwork for publication in third party publications (e.g. Green and White magazine, local and national newspapers, FAI/GAA websites).

If you do not wish to have your child's photograph/video/schoolwork used in any form, please put this information in writing to the school Principal. If, at any stage, you change your mind, it is your responsibility to notify the school in writing.

Parent/Guardian Signature: _________________________ Date: ___________________

Appendix 2

Stop Cyber bullying

Tips for Parents

It is very important that you listen to your child when they come to you with an issue relating top bullying.

Encourage your child to be careful about disclosing personal information.

Being conscious of when and where it is all right to reveal personal information is vital. A simple rule could be that the child should not give out name number or picture without your approval. Never give out personal information (PIN) etc. online everyone is a stranger. Don't talk to or accept anything from strangers.

Remember that the positive aspects of the Internet and Mobile Phones outweigh the negatives. The Internet is an excellent educational and recreational resource for children. Mobile phones can be a source of comfort and support for children and parents.

Know your child's net use.

To be able to guide your child with regard to Internet use, it is important to understand how children use the Internet and know what they like to do online. Let your child show you which websites they like visiting and what they do there.

Encourage good Netiquette

Netiquette is the informal code of conduct for the Internet. These are informal ethical rules for how to behave when relating to other people on the Internet and include: being polite, using correct language, not yelling (writing in capital letters) not harassing others or provoking fights online. You should not read other's email or copy protected material.

Some Tips for Young People.

Do trust your instincts. If it doesn't look or feel right it probably isn't. If you find something online that you don't like or makes you feel uncomfortable, turn off the computer and tell an adult.

Do not keep this to yourself! You are NOT alone! Tell an adult you know and trust!

Do not delete messages from cyber bullies. You don't have to read it, but keep it, it is your evidence.

Don't send a message when you are angry. Wait until you have time to calm down and think. You will usually regret sending a "Flame" (angry message) to someone else. Once you've sent a message, it is very hard to undo the damage.

Don't open messages from people you don't know.

Don't reply to messages from cyber bullies! Even though you may really want to, this is exactly what the cyber bullies want. They want to know that they've got you worried and upset. They are trying to mess with your mind and control you, to put fear into you. Don't give them that pleasure.

What to do if you are cyber bullied.

- Tell your parents or a trusted adult.

- Do not retaliate – this will only feed into the cyber bully and could make other people think you are part of the problem.

- Try to ignore the cyber bully.

- Block the bully from your site.

- Save the evidence. Keep a record of the bullying messages but do not reply to any bullying messages.

- Show or give the record of bullying messages to your parents.

If the cyber bullying persists or gets worse, your parent or trusted adult can:

- File a complaint with the website, ISP, or Mobile Phone Company. There is usually a link on the website's home page for reporting concerns.

- Contact the Gardaí if the cyber bullying contains any threats.

Appendix 3

St. James' N.S. Rules for Responsible Internet Use

The school has installed computers with Internet access to help our learning. These rules will help keep us safe and help us be fair to others.

Using the computers:

1. I will not access other people's files;
2. I will not use CD-ROMs, memory sticks, cameras, iPads, laptops, mobile phones or MP3 players without the permission of the teacher;
3. I will treat all of the computer equipment with respect.

Using the Internet:

1. The use of the Internet is for educational purposes only;
2. I will not use the Internet, unless given permission by a teacher;
3. I will report any unpleasant material to my teacher immediately because this will help protect other pupils and myself;
4. I understand that the school may check my computer files and may monitor the Internet sites I visit;
5. I will not complete and send forms without permission from my teacher;
6. I will not give my full name, my home address or telephone number when completing forms or while visiting websites;
7. I will not upload or download non-approved material.

Using e-mail:

1. I will ask permission from a teacher before checking the e-mail;
2. I will immediately report any unpleasant messages sent to me because this would help protect other pupils and myself;
3. I understand that e-mail messages I receive or send may be read by others;
4. The messages I send will be polite and responsible;
5. I will only e-mail people I know, or my teacher has approved;
6. I will only send an e-mail when it has been checked by a teacher;
7. I will not give my full name, my home address or telephone number or that of anyone else;
8. I will not send or open attachments without the permission of the teacher.

I understand that failure to comply with the rules will mean withdrawal of Internet privileges.

Signed: ________________________ Class: ________________________

Date: ________________________

Appendix 4

St. James' NS- Ipad Code of Behaviour

The purpose of this code is to govern the use of iPads by students in our school. This code is informed by and serves as an extension of the following School policies:

- Code of behaviour
- ICT Acceptable Usage Policy

Respect is the fundamental core principle upon which this code of behaviour is based. The role of the iPad in the school context is a tool to support learning.

General iPad Rules:

1. The school reserve the right to decide on the appropriateness of available Apps. Any Apps deemed inappropriate will not be permitted on students iPads. Students and their parents will be advised of prohibited Apps. Snapchat is prohibited.
2. Students are strictly prohibited from inappropriate use of the camera on the iPad. No video, image or audio recording are to be taken unless specified and supervised by a teacher. Breaching this rule is a serious disciplinary offence and may result in suspension.
3. The images, videos, music and apps. on a students Ipad must be must be appropriate and in keeping with the school's ethos. Sharing inappropriate material, images or videos is a serious disciplinary offence.
4. Students may not use their iPads to communicate with each other, unless directly instructed to do so by a teacher, during the school day.
5. An MDM (multi device management) profile called Mosyle profile has been installed on all iPads by iConnect at deployment. Students are not permitted to remove it.
6. iPads are not to be used in between classes or at break times or at any time where the teacher has instructed the class not to use them.
7. All iPads must be stored in the assigned storage box.
8. Students are responsible for the safety and protection of the iPad and that it is kept away from liquids or likely damage.

iPad Classroom Rules:

1. iPads are only to be used for Educational use and in adherence with the School's Acceptable Usage Policy and as directed by the classroom teacher.
2. Only the apps specified by the classroom teacher are to be open.
3. The iPad should be kept flat on the desk at all times.
4. Students should close all apps at the end of each class.
5. No video, image or audio recording are to be taken unless specified by the classroom teacher.
6. Students may not use the iPad to communicate with each other during the class unless requested to do so by their teacher
7. Audio output from your Ipad is only permissible when requested by the classroom teacher.

Appendix 5

Support Structures

The following are some useful websites. Please note that these links are intended as assistance and St. James' NS does not accept responsibility or endorse any of the websites listed nor the information that is contained within them.

www.internetsafety.ie

www.rollercoaster.ie

Office for internet Safety Advice for parents

www.watchyourspace.ie

Advice on managing children's profiles on social-networking

www.webwise.ie

Provides parents, teachers, and children with educational resources, advice and information about potential dangers on the internet websites

www.scoilnet.ie

Provides advice and support to schools on Information Technology

www.netsecure.ie

National awareness campaign on computer security

www.equality.ie

The Equality Authority

Sanctions

www.makeitsecure.org

Provides information on IT security risks on line

www.childline.ie

Child Safety issues

www.hotline.ie

Irish hotline for public to report child pornography and other illegal content

www.barnardos.ie

Charity for the protection of children

www.ncte.ie

The National Centre for Technology in Education provides advice and support on ECTs in education

http;//www.ec.europa.eu/ information society/activities/ sip/safety tips/index en.htm A European Union website with safety tips on social-networking.