**St. Brendan’s NS Acceptable Use Policy June 2020**

**Rationale:**

This policy is a revision of the school’s previous AUP policy. It was updated to take into account the rapid developments in online teaching and learning that have taken place during the Covid 19 school closure period 2020.

The school, up to that point, had a G Suite account but had been making only basic use of it as a communication and collaboration tool for teachers. Teachers had been assigned G-mail addresses but not pupils. Kahoots and Class Dojo were used by senior classes. ASD teachers and parents had been making daily use of the See Saw app as a home-school communication device. Our website was outdated and our Facebook Page under-used. Communication between home and school was traditionally by post and text-a-parent messages.

As a result of the school shutdown, the staff moved quickly to the everyday use of Google Classrooms and associated tools in G Suite and a range of other online teaching platforms, including Padlet, Zoom and Kahoots. A professionally-designed school website and app for parents was developed rapidly during this period also.

 E-mail communication between home and school has become the norm. Children are encouraged to use Google Docs, scanned attachments, photos and video clips to return work. Links to interactive educational websites, You Tube, online spelling/reading/maths sites that gather attainment data have become an everyday reality and will continue to do so into the future. We plan to build on this foundation and assign e-mail addresses to all pupils in the school so that the full range of G Suite apps can be used securely within the school community. We will also be moving towards the compilation of e-portfolios for each pupil saved on the school’s Google Drive.

While we are pleased that a huge leap in the attainment of IT skills has been made by all stakeholders in our school community, this revised policy is needed now to ensure that the ground rules are updated to protect the safety of all concerned in this new way of teaching and learning.

**What devices does the policy apply to:**

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

**Who the policy applies to:**

 This Policy applies to staff, students and parents of St. Brendan’s 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.

**Aim:**

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 Internet Safety Protocols**

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. ( see note in appendix 1 and 2 below)
* Pupils and teachers will be provided with training 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.
* Pupils will take part in Webwise activities in February each year as part of the school’s SPHE plan and from time-to-time at assemblies throughout the year as the need arises.
* 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.
* The school appoints an ICT co-ordinator as part of the in-school management team to oversee all policies in regard to ICT and digital learning within the school.

***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**

* Pupils will be taught specific lessons on online safety by teachers.
* Pupils 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 pupil 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.
* Pupils 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.
* Pupils will not examine, change or use another person’s files, username or passwords.
* Pupils 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, pupils will use approved class email accounts or parent-accounts under supervision of a teacher or parent/guardian.
* Parents will be appropriately informed about G Suite and other learning platforms being used in the school and required to sign that pupils have their permission to use G Suite
* Parents will be able to log-in and monitor their child’s use of G Suite and other digital learning platforms.
* Pupils will not send or receive any material that is illegal, obscene, defamatory, or that is intended to annoy or intimidate another person.
* Pupils will not reveal their own or other people’s personal details, such as addresses or telephone numbers or pictures.
* Pupils will never arrange a face-to-face meeting with someone they only know through emails or the Internet.
* Pupils will note that sending and receiving email attachments is subject to permission from their teacher

**Distance Learning /Flipped Classroom**

In circumstances where teaching cannot be conducted on the school premises, teachers may use Google Classroom, Google Meet, Zoom, SeeSaw, Kahoots, Padlet, Class Dojo, Mentimeter or other platforms approved by the Principal as platforms (the “Online Platforms”) to assist with remote teaching where necessary. See appendix 3

Digital learning platforms will continue to be integrated with face-to-face teaching to enhance the overall learning experience of our pupils and prepare them for life and work in the 21st century. A flipped classroom is a [type of blended learning](https://www.teachthought.com/learning/12-types-of-blended-learning/) where students are introduced to content at home and practice working through it at school. This is the reverse of the more common practice of introducing new content at school, then assigning homework and projects to completed by the students independently at home. In this blended learning approach, face-to-face interaction is mixed with independent study–usually via technology. In a common Flipped Classroom scenario, pupils might watch pre-recorded videos at home, then come to school to do the homework armed with questions and at least some background knowledge.

* 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@stbrendanscartron.com.
* 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.
* Parents/guardians must also agree to monitor their child’s participation in any such lessons conducted on the Online Platforms.

**Internet Chat**

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

**Virtual Class Meetings eg Zoom, Skype or Google Meet etc**

* If teachers are using Zoom or Google Meet parents/guardians must consent to their child having a school- assigned 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.

Teachers should adhere to the following agreed protocols-

* Two adults need to co-host in case the main host's connection drops and pupils continue the meeting unsupervised.
* Test audio and video beforehand.
* Set up a waiting room to control access.
* Agree conditions and sanctions with pupils before the meeting.
* Use mute button to only allow pupils to speak when invited by teacher.
* Lock meeting after all participants are present to avoid any unwanted visitors.
* Meeting should be password protected and teacher needs to ensure all prospective participants have been given the correct access codes. Use text message to share this information if necessary to reach the full class.
* Use share screen facility to give a talk over if preferred to appearing live on video.
* Take care of the appropriateness of your own background. Use a pre-selected background if necessary.
* Be very clear how to mute and un-mute participants in the event of inappropriate behaviour or background noises.
* Know how to eject a participant from a meeting in the event of inappropriate behaviour.
* Ensure your or participants email address, other personal details or inappropriate web pages are not visible especially when screen sharing.
* Meeting cannot be recorded by host or participants without consent from all. Know how to identify if any participants have pressed record.
* Have a procedure in place for participants who may be stuck in the waiting room or whose connection drops and wish to re-enter the meeting eg use another device to monitor email or messages on Google Classrooms from participants having technical difficulties.
* Establish ground rules with participants and parents in advance
* Chat facility should not be used with younger participants

Pupils should-

* Adhere to an appropriate dress code (e.g. no pyjamas or hoodies blocking faces)
* Not eat or drink during the meeting, for reasons of safety and courtesy
* Not have other phones, digital or recording devices in their hands during the meeting
* Do not leave the camera or walk around with the device still broadcasting
* Do not turn off video deliberately mid-meeting, unless in the event of an unforeseen emergency
* Ensure pets or younger siblings cannot interrupt the meeting or interfere with devices
* Parents should be present for children up to age 8
* Older siblings eg teenagers should only be present with the parent and teachers consent
* No recording of the session
* Hand up to speak or use hand icon
* Follow the rules set down by the teacher
* Sanctions for not following the rules will include being muted by the teacher, being ejected from the meeting, banned from further meetings, red/yellow card and sanctions from the school behaviour code up to and including suspension or expulsion for gross misbehaviour during the conference call

**School Website and affiliated Social Media sites, School App.**

* The school’s website address is: [www.stbrendanscartron.com](http://www.stbrendanscartron.com)
* The School’s Facebook account is: <https://m.facebook.com/StBrendansNS>
* The school uses an app affiliated with the website hosted by Schools Ireland
* Pupils 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.
* All material uploaded to the website must be approved by the designated administrators. Upload is blocked until approval is given.
* 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.
* Photographs, audio and video clips will focus on group activities, where children will not be named.
* 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. Children in photographs will not be identified by name.
* Photos/Videos may be used for the production of school booklets 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 ICT Co-ordinator, website Co-ordinator and Principal will have administrative and editorial access to the website. No materials can be published without the permission of these administrators.
* The ICT Co-ordinator, website Co-ordinator and 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 and Taking & Use of Photographs Policy.***

**Personal Devices**

* Pupils 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 smart-phones or other personal devices must be downloaded onto the Google Drive , designated school external hard drive and/or on to the school App/relevant school affiliated website and then immediately deleted from source.

**Legislation and Regulation**

On request, the school will provide information on the following legislation relating to use of the Internet with which teachers, pupils 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.

**Education of pupils on how to be safe online and when using ICT**

* The school has purchased several workbooks and teacher guidelines with regard to educating children about the safe use of the internet.
* Cyberbullying is recognised in our school Anti-bullying Policy and Behaviour Code.
* We will be accessing suitable materials on [www.webwise.ie](http://www.webwise.ie) and the [www.saferinternetday.ie](http://www.saferinternetday.ie) which have been specially designed for use in a school setting.
* On an annual basis in February, 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.

**Pupil and Staff Use of Information Communication Technology (“ICT”) Resources**

St. Brendan’s NS’ ICT devices and systems (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.

* As school property, permission must be sought before removing the devices from the premises.
* All devices they must be returned immediately to the school upon request.
* 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. These devices are for school related activities only.
* 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.
* Downloading software programmes must be reported to the ICT co-ordinator in advance and permission given before download takes place.
* No alteration to the devices operating system is permitted without consultation with the school’s ICT co-ordinator.
* Material damage to the device must be reported to the ICT Co-ordinator immediately and no repairs undertaken without the school’s permission.
* 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”).

**ICT Co-ordinator’s Role**

* The ICT Co-ordinator will compile “best advice” sheets for teachers and parents based on the current best-practice and focussing particularly on security and safety.
* The ICT Co-ordinator and Principal will have admin access to G Suite and whatever other distance learning platforms are being used in the school and will be signed up as “co-teacher” to monitor and advise on safe use of these platforms. The co-ordinator can switch on/off elements within G Suite and other platforms to enhance security and safety for pupils and staff.
* The ICT Co-ordinator and Principal will ensure that all staff have regular training on all the distance learning platforms currently in use in the school. Suitable training has been identified through PDST and Scoilnet: <https://www.scoilnet.ie/tools-for-teachers/articles/eportfolio/>
* Maintain the school devices, ensuring nothing inappropriate has been saved on the device.
* Ensure that all necessary parental permission has been obtained. Maintain a record of pupils whose parents have not granted permission for all or any of the areas covered in this policy.
* Ensure that all new staff members are furnished with a copy of this policy immediately upon commencing work in St. Brendan’s NS
* Has administrative access and control in conjunction with the Principal and Website Administrator to all school devices, G Suite and other digital learning platforms
* The ICT co-ordinator will ensure that pupils are given regular education in relation to the safe and appropriate use of digital devices, email, social media and the internet.

**Sanctions**

Misuse of the Internet, school devices 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.

**Success Criteria:**

* Parents, pupils and staff of St. Brendan’s will continue to develop digital learning capacity and skills in line with modern trends and best practice
* Teaching and learning will be enhanced
* Digital devices and platforms will be used regularly and appropriately
* Pupils, parents and teachers will have a high degree of confidence that personal safety and security is to the forefront of all digital learning

**Ratification and communication:**

* This AUP will be distributed to staff, parents, Parents’ Association and Board of Management for comment and alteration if necessary.
* It will be ratified by the Board of Management and published on the school website and in the parental handbook.
* The Policy will be reviewed annually as this is a rapidly developing and changing area of education.
* Parental permissions must be sought on enrolment but also as the need arises when new technology and digital learning platforms become available.

**Acceptable Use Policy Permission Slip**

Dear Parent(s)/Guardian(s), The staff and Board of Management of St. Brendan’s 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.

Name of pupil: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Class/Year: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Parent/Guardian,

As the parent or legal guardian of the above student, I have read the Acceptable Use Policy and grant permission, within the parameters set out in the policy, for my child to (please tick):

* access the Internet in school
* use school digital devices
* have his/her work published to the school’s website
* have his/her photograph/video in a group setting published to the school’s website, app and social media
* Have his/her individual photograph/video published to the school’s website, app and social media
* Have his/her individual photograph/video published in local or national media eg local or national newspaper
* use an assigned school email address for the purpose of accessing the G Suite for education apps
* have his/her work saved on the school’s Google Drive

I understand that students may not be able to participate fully in lessons involving PCs, laptops, iPads, tablets and other IT equipment without consenting to our Acceptable Use Policy.

*All of the above are to the school’s GDPR, Anti-Bullying and Child Protection Policies.*

 Parent/Guardian Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Appendix 1**

**Filtering**

The Schools Broadband Network operates the FortiGuard Web Filtering Service from Fortinet. This is a hosted service designed to provide Web URL filtering for schools, libraries, government agencies and enterprise businesses of all sizes. What this means is that websites accessed on the Schools Broadband Network go through a level of filtering to ensure that inappropriate sites are excluded and a "Web  Page Blocked" message is displayed.

Fortinet is a member of the Internet Watch Foundation in the UK working to combat potentially illegal online content and prevent access to child sexual abuse. Fortinet's Web Filtering Solutions are also CIPA certified. The Children's Internet Protection Act (CIPA) is a federal law enacted by US Congress in December 2000 to address concerns about access in schools and libraries to the Internet and other information.

Websites are categorised into one of 76 categories and access to a website is conditioned on the category being available to the school. Currently schools have the choice between two options A and B as to what categories are available for access within their school. Option B: a restrictive level which permits only educational websites as well as sites on a pre-determined 'white list'; and Option A is a less restrictive system which allows other websites in addition to what is available on option B. [Filtering Categories v2](http://www.ncte.ie/documents/broadband/FilteringCategoriesv2.pdf) lists the available categories and which category is included within the two options.

Despite having some 30 million websites categorised it is possible that a website may be uncategorised or unrated. Where this is the case it is possible to suggest a category for this website to the filtering system. This can be done through the following link:

[**Fortinet**](http://www.fortiguardcenter.com/webfiltering/webfiltering2.html)

The system is automated and usually responds within 24 hours. Once the website is categorised, and assuming it does not come under the blocked categories, it should be possible to view the website on the Schools Broadband Network.

Where a website is in a category not allowed on the Schools Broadband Network but it is deemed that the website should be made available to schools, that website may be added to a Whitelist. All websites listed in the Whitelist are made available to schools. Where a website is in a category that is allowed on the Schools Broadband Network but it is deemed that the website is not appropriate for schools, that website is added to a Blacklist. All websites listed in the Blacklist are not accessible in schools.

Schools may switch between option A and B by filling out the [Content Filtering Option form](http://www.ncte.ie/documents/broadband/CF1Formv3.pdf) and returning it to the Service Desk.  Schools may request that a website be reviewed for adding to the whitelist or blacklist by contacting the [Service Desk](http://www.ncte.ie/servicedesk).

**Appendix 2 NCTE Service Desk, P.O. Box 10101, Dublin 17.**

 Or completed forms may be **faxed to 01- 8473370**

**Confirmation of Content Filtering Option (CF1 form, version 3)**

***Please complete this form which is required for the selection of a Content Filtering option for your school.***

***If you have any queries in relation to this form, please call the NCTE Service Desk on free phone 1800 33 44 66.***

|  |
| --- |
| **School Roll Number**  |
| **School Name**  |
| **School Address**  |
| **Content Filtering Option**  | ***Tick the appropriate box to indicate the filtering option required. (tick one box only)***  |
| **Option A:** This option allows access to a wide range of websites and categories, while blocking potentially liable, objectionable or controversial content.  | 􀂆Yes  |
| **Option B:** This option allows access to a more restricted range of educational and cultural websites.  | 􀂆Yes  |

**As Principal I confirm the following on behalf of the school:**

1. 1. The school has completed and returned the ‘Confirmation of School Internet AUP’ Form (CAUP1 form) to NCTE Service Desk.
2. 2. The School understands and accepts that online use via the Schools Broadband Network will be monitored by the Schools Broadband team.
3. 3. School Authorities will inform staff and students that Internet and email use will be monitored and that inappropriate use of the service may result in sanction by the school.
4. 4. The School understands and accepts that where a school is considered to be a risk to the schools broadband network, or is engaging in inappropriate online behaviour the Broadband Schools team reserve the right to take whatever actions are required to protect the network and other schools. This may require disconnecting the ‘offending school’ until the situation is resolved satisfactorily.

**Signed by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**(Principal)**

**Principal’s Name *(in capitals****)*: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date:** \_\_\_\_\_\_\_\_\_\_\_\_

*Please return this signed form to*

**Appendix 3**

### [About G Suite](https://www.scoilnet.ie/fileadmin/user_upload/Google_Forms_.pdf)

<https://www.scoilnet.ie/tools-for-teachers/articles/eportfolio/>

G Suite is a combination of free **ONLINE** productivity tools for classroom collaboration. The system is very quick and easy to set up. Organisation is key across ALL ePortfolio platforms and the skill of management is required.
Tools include;

* **Google Classroom** - an online classroom for teachers to organise classroom resources for class, create & organise assignments, communicate with the class, provide feedback and answer student questions when they online.
* [**Google Drive**](http://pdst.ie/sites/default/files/How%20to%20use%20Google%20Drive.pdf)**-** Unlimited cloud storage where students and teachers can upload files/folders from computer or organise Google Docs, Sheets and Slides. Students can share their folder with their teachers. Students can share folders with other students during group-work tasks.
* **Google Docs and Slides** - Students can create online documents using Google Docs and presentations using Google Slides. A very nice feature within Google Docs/Slides is the collaboration function, students can share and edit files in real-time - the whole class could be working on one document. Image searches within Google Docs/Slides return images which comply with safesearch and approved for use with Creative Commons.
* **Google Sheets**- Students can create spreadsheets. Spreadsheets can also be shared with other students/teacher to collaborate on one piece of work together at the same time. A clever feature within Google Sheets is how Google Sheets can create formulas from student questions.
* **Google Scheduling** - Google Calendar can suggest available times to meet other teachers 1:1 and even suggest available rooms. Upcoming school events can be easily shared with students and teachers
* [Google Forms](https://www.scoilnet.ie/fileadmin/user_upload/Google_Forms_.pdf) - Students/ teachers can create questionnaires or surveys for class to complete. There are various questions type such as text, paragraph, multiple choice, checkboxes, scale and grid...etc.

**About See Saw**

Seesaw is a free platform where students can create ePortfolios to document their learning journey. Students will take ownership of their ePortfolios as their portfolio grows and their digital skills progress. Seesaw is a particularly nice platform for primary school students and learning resource classes. There are some extremely useful tools within Seesaw. One such tool is the ability to record. Students can record their own voice to set personal reminders or advice. The ability to record enables differentiation within instruction formats and enables all students to organise their learning around their preferred learning style.

Seesaw is excellent for monitoring and reviewing developmental progress in learning. Teachers and learning support teachers can strengthen their educational and professional relationship along with supporting pupils/students challenges and celebrating pupils/students achievements. All eportfolios on Seesaw are password protected but the teacher can provide a QR code to parents which will give them access to their own child’s eportfolio of work. With Seesaw, teachers will hear students asking ‘Are you going to show my parents my work?’

### [About Padlet](https://padlet.com/)

A virtual online wall where students can share their learning or prior knowledge collaboratively with the class. Students can present their understanding onto the online wall using text, image, video or in document format. New feature on Padlet enables students to create flow charts and connect posts with arrows.

**To parents and guardians,**

At St. Brendan’s NS we use G Suite for Education, and we are seeking your permission to provide and manage a Google Classrooms and G Suite account for you/your child. G Suite for Education is a set of education productivity tools from Google including Gmail, Calendar, Docs, Classroom, and more used by tens of millions of students and teachers around the world.

At St. Brendan’s, students will use their Google classroom accounts to complete assignments and communicate with their teachers. In the future we may use some of the other tools available through G Suite for Education, including giving individual email addresses to pupils for this purpose.

The notice below provides answers to common questions about what Google can and can’t do with your child’s personal information, including:

* What personal information does Google collect?
* How does Google use this information?
* Will Google disclose my child’s personal information?
* Does Google use student personal information for users in Primary schools to target advertising?
* Can my child share information with others using the G Suite for Education account?

Please read it carefully, let us know of any questions.

I give permission for St. Brendan’s NS to create/maintain a G Suite for Education account for my child and for Google to collect, use, and disclose information about my child only for the purposes described in the notice below.

**You can email your consent to** **secretary@stbrendanscartron.com** **. However, in the event that we do not receive an email of consent, we will take your accessing of the Google Classroom materials to be an acknowledgement of your consent.**

**We will also send a text message to all families giving an option to opt out of Google Classrooms/G Suite by email.**

Thank you,
Marie Hurley

G Suite for Education Notice to Parents and Guardians

This notice describes the personal information we provide to Google for these accounts and how Google collects, uses, and discloses personal information from students in connection with these accounts.

Using their G Suite for Education accounts, students may access and use the following “Core Services” offered by Google (described at <https://gsuite.google.com/terms/user_features.html>):

* Gmail
* Google+
* Calendar
* Chrome Sync
* Classroom
* Cloud Search
* Cotacts
* Docs, Sheets, Slides, Forms
* Drive
* Groups
* Hangouts, Hangouts Chat, Hangouts Meet, Google Talk
* Jamboard
* Keep
* Sites
* Vault

https://support.google.com/a/answer/6356441In addition, we may also allow students to access certain other Google services with their G Suite for Education accounts e.g. YouTube, Blogger, Google Maps.

A list of additional services is available at <https://support.google.com/a/answer/181865>, and instructions for administrators about how to enable or disable them are available at <https://support.google.com/a/answer/182442>.]

Google provides information about the information it collects, as well as how it uses and discloses the information it collects from G Suite for Education accounts in its G Suite for Education Privacy Notice. You can read that notice online at <https://gsuite.google.com/terms/education_privacy.html> You should review this information in its entirety, but below are answers to some common questions:

What personal information does Google collect?

When creating a student account, St. Brendan’s NS may provide Google with certain personal information about the student, including, for example, a name, email address, and password. Google may also collect personal information directly from students, such as telephone number for account recovery or a profile photo added to the G Suite for Education account.

When a student uses Google services, Google also collects information based on the use of those services. This includes:

* device information, such as the hardware model, operating system version, unique device identifiers, and mobile network information including phone number;
* log information, including details of how a user used Google services, device event information, and the user's Internet protocol (IP) address;
* location information, as determined by various technologies including IP address, GPS, and other sensors;
* unique application numbers, such as application version number; and
* cookies or similar technologies which are used to collect and store information about a browser or device, such as preferred language and other settings.

How does Google use this information?

In G Suite for Education Core Services, Google uses student personal information to provide, maintain, and protect the services. Google does not serve ads in the Core Services or use personal information collected in the Core Services for advertising purposes.

[Include this section if your school provides access to Additional Services] In Google Additional Services, Google uses the information collected from all Additional Services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and its users. Google may also use this information to offer tailored content, such as more relevant search results. Google may combine personal information from one service with information, including personal information, from other Google services.

Does Google use student personal information for users in Primary schools to target advertising?

No. For G Suite for Education users in primary and secondary schools, Google does not use any user personal information (or any information associated with an G Suite for Education Account) to target ads, whether in Core Services or in other Additional Services accessed while using an G Suite for Education account.

Can my child share information with others using the G Suite for Education account?

[As applicable for school/district] We may allow students to access Google services such as Google Docs and Sites, which include features where users can share information with others or publicly. When users share information publicly, it may be indexable by search engines, including Google.

Will Google disclose my child’s personal information?

Google will not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances applies:

* With parental or guardian consent. Google will share personal information with companies, organizations or individuals outside of Google when it has parents’ consent (for users below the age of consent), which may be obtained through G Suite for Education schools.
* With [insert name of school/district]. G Suite for Education accounts, because they are school-managed accounts, give administrators access to information stored in them.
* For external processing. Google may provide personal information to affiliates or other trusted businesses or persons to process it for Google, based on Google’s instructions and in compliance with the G Suite for Education privacy notice and any other appropriate confidentiality and security measures.
* For legal reasons. Google will share personal information with companies, organizations or individuals outside of Google if it has a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:
	+ meet any applicable law, regulation, legal process or enforceable governmental request.
	+ enforce applicable Terms of Service, including investigation of potential violations.
	+ detect, prevent, or otherwise address fraud, security or technical issues.
	+ protect against harm to the rights, property or safety of Google, Google users or the public as required or permitted by law.

Google also shares non-personal information -- such as trends about the use of its services -- publicly and with its partners.

What choices do I have as a parent or guardian?

First, you can consent to the collection and use of your child’s information by Google. If you don’t provide your consent, we will not create a G Suite for Education account for your child, and Google will not collect or use your child’s information as described in this notice.

If you consent to your child’s use of G Suite for Education, you can access or request deletion of your child’s G Suite for Education account by contacting [insert contact information for school administrator]. If you wish to stop any further collection or use of your child's information, you can request that we use the service controls available to limit your child’s access to features or services, or delete your child’s account entirely. You and your child can also visit [https://myaccount.google.com](https://myaccount.google.com/) while signed in to the G Suite for Education account to view and manage the personal information and settings of the account.

What if I have more questions or would like to read further?

If you have questions about our use of Google’s G Suite for Education accounts or the choices available to you, please contact [insert contact information for the school administrator]. If you want to learn more about how Google collects, uses, and discloses personal information to provide services to us, please review the [G Suite for Education Privacy Center](https://www.google.com/edu/trust/) (at https://www.google.com/edu/trust/), the [G Suite for Education Privacy Notice](https://gsuite.google.com/terms/education_privacy.html) (at https://gsuite.google.com/terms/education\_privacy.html), and the [Google Privacy Policy](https://www.google.com/intl/en/policies/privacy/) (at https://www.google.com/intl/en/policies/privacy/).

The Core G Suite for Education services are provided to us under [Google’s Apps for Education agreement](https://www.google.com/apps/intl/en/terms/education_terms.html) (at https://www.google.com/apps/intl/en/terms/education\_terms.html) [if school/district has accepted the Data Processing Amendment (see <https://support.google.com/a/answer/2888485?hl=en>), insert: and the [Data Processing Amendment](https://www.google.com/intl/en/work/apps/terms/dpa_terms.html) (at https://www.google.com/intl/en/work/apps/terms/dpa\_terms.html)].