St Joseph's Patrician College, Galway.
'THE BISH'

Acceptable Use Policy with Mobile Phone (AUP)

Policy Revision Number:	Date.
1	24th May. 2021
2	05/11/2021

Ratification Date: 5th November 2021

This policy is in keeping with the Child Protection Procedures as adopted by the Board of Management. Teachers are reminded that they are mandated persons and must be familiar with their obligations with reference to the Children first: National Guidance for Protection and Welfare of Children 2017 and the Children First Act 2015

The policy applies to all students and to all personnel employed in St Joseph's Patrician College.

Rational

The aim of this Acceptable Use Policy (AUP) is to ensure that students and staff will benefit from learning opportunities offered by St Joseph's Patrician College's Internet resources in a safe and effective manner.

Internet use and access is considered a St Joseph's Patrician College resource and privilege. Therefore, if the St Joseph's Patrician College AUP is not adhered to, this privilege will be withdrawn and appropriate sanctions –as outlined in the AUP will be imposed.

This policy was devised locally following a comprehensive review of the opinions, experiences and concerns of our community of students, staff and parents, recorded through a series of surveys, focus group discussions and in consultation with the Students Council 2020-2021 regarding access to and use of mobile devices in the school context.

Mobile devices/phones have become an important and invaluable part of our modern lifestyle.

The school understands that at times, where deemed necessary by parents/guardians the possession of a mobile phone can provide a sense of safety and security for students travelling to and from school.

Within the school site and in the course of the school day this policy aims to maintain a safe, secure and nurturing environment where the personal dignity and rights of all the members of the school community are preserved and protected.

The policy has also been influenced by the focus on this issue at National policy level. The Department of Education and Skills Circular 0038/2018 emphasises that centrality of this issue to school communities nationwide.

Basic Principles:

This policy is a school-wide policy, arrived at through engagement with all members of our school community. The policy encourages the personal management of mobile devices and requires the support of all staff, students, parents and Board of Management. The policy is inextricably linked to a number of other policies in the school – The Code of Behaviour, St. Joseph's Patrician College AUP, Child Protection Safeguarding Statement (and associated policies), Dignity in the Workplace, etc.

This AUP will be revised as it becomes necessary.

Objectives:

The school aims to provide a happy, safe supportive and inclusive learning environment for all students. The purpose of this policy is to:

•Clearly set-out and explain the agreed policy regarding access to and use of internet resources and mobile devices in St. Joseph's Patrician College.

- Ensure that access to internet resources and mobile device usage does not disrupt this learning environment.
- Support the wellbeing and dignity of all students and all staff.
- Ensure that courtesy to, respect and consideration of others are paramount at all times
- ***Clarify the responsibilities of students and staff with regard to internet resources and mobile devices and the*** conditions associated with students bringing their mobile phones to school:

"…. young people need to be guided and supported to become

good digital citizens. In a school setting, using digital

technologies mediated by the teacher with the skills to exploit

the potential of the technologies can be invaluable in

equipping children with the skills to navigate the online world

safely."

DES, Circular 0038/2018

We welcome, care for and support all within the school community through the promotion of:

- Respect
- Being just & responsible
- Quality teaching and learning

• An inclusive community

• Life-long learning

St Joseph's Patrician College's Strategy for Internet Resources.

St Joseph's Patrician College will employ a number of strategies in order to maximize learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

General:

1. Student Internet sessions will always be supervised by a teacher.
2. Filtering software and/or equivalent systems will be used in order to minimize the risk of exposure to inappropriate material.
3. The Teacher will regularly monitor students' Internet usage.
4. Teachers and students will be provided with guidelines in the area of Internet safety.
5. Uploading and downloading of inappropriate software will not be permitted.
6. Virus protection software will be used and updated on a regular basis.
7. The use of personal USB sticks or CD-ROMs or other external memory devices in St Joseph's Patrician College by students is not permitted.
8. Users will observe good "netiquette" (i.e., etiquette on the Internet) at all times and will not undertake any actions that may bring the St Joseph's Patrician College into disrepute.
9. All students enrolled in St Joseph's Patrician College will have access to a Microsoft office 365 account. This account will be the main platform for IT use in the school.

World Wide Web

1. Users will not visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
2. If in doubt about the suitability of a site, the student must bring it to the attention of the teacher immediately.

3. Students will use the Internet for educational purposes only. Students will be made aware of copyright issues relating to online learning.
4. Students will never publicize personal information unless in the context of approved educational use.
5. Users will be aware that any usage, including distributing or receiving information, of St Joseph's Patrician College related material or personal, may be monitored for unusual activity, security and/or network management reasons.

Email

1. All students will be allocated a @bish.ie email account and password. This account will remain the property of the St Joseph's Patrician College and will be monitored by the St Joseph's Patrician College authorities. Students must be aware that all accounts will be supervised and maintained by St Joseph's Patrician College.
2. The St Joseph's Patrician College @bish email address is for St Joseph's Patrician College and educational purposes only.
3. Students will not send or receive any material that is illegal, that contains virus, is obscene, defamatory or that is intended to annoy or intimidate another person or is inappropriate in any way.
4. If any unacceptable behaviour is suspected or reported, St Joseph's Patrician College has the right to access, edit, delete or block a student's St Joseph's Patrician College email account.
5. Students cannot change their email account password. If necessary this will be done by the relevant St Joseph's Patrician College authority.
6. Students will not reveal their own or other people's personal details, such as addresses, passwords, telephone numbers or photographs.
7. Students will never arrange a face-to-face meeting with someone they only know through emails or the internet.
8. Students may only email teachers or members of the staff with the direct permission of the relevant teacher or member of staff, and then only using an @bish email address.
9. Students will note that sending and receiving email attachments is subject to permission from their teacher.
10. The email address will be valid only for the duration of the student's time in St. Joseph's College.

11. Students are responsible and accountable for any communications or activities associated with their St Joseph’s Patrician College email addresses. They should therefore ensure the privacy of their passwords.
12. Profile pictures must be appropriate for a school account and deemed appropriate by teachers who may be required to view profile pictures.

Internet Chat

1. Students will only have access to chat rooms, discussion forums or other electronic communication forums that have been approved by St Joseph’s Patrician College and with permission from and supervision by a teacher.
2. Chat rooms, discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.
3. Face-to-face meetings with someone organized via Internet chat will be forbidden.

St Joseph’s Patrician College, Website

1. Students’ may be given the opportunity to publish projects, artwork or St Joseph’s Patrician College work on the World Wide Web.
2. The publication of student work will be co-coordinated by a teacher.
3. Students’ work will appear in an educational context on Web pages with a copyright notice prohibiting the copying of such work without express written permission.
4. Digital photographs, audio or video clips of individual students will not be published on the St Joseph’s Patrician College website.
5. Instead photographs, audio and video clips will focus on group activities.
6. Video clips may be password protected. Personal pupil information including home address and contact details will be omitted from St Joseph’s Patrician College web pages.
7. Students will continue to own the copyright on any work published.

St Joseph’s Patrician College’s Strategy for Mobile Phones

This strategy applies to the entire school campus which includes the school buildings, environs and all school related activities that occur on-site and off-site in the name of the school.

- If mobile phones are brought to school, the school accepts no responsibility for replacing lost, stolen or damaged mobile phones. The safety and security of mobile phones is wholly a matter for students / parents.
- If brought to school mobile phones must be stored throughout the day in students school bag /secured in student locker so as not to disrupt learning and teaching in class. **It is the student's responsibility to make sure their phone does not disturb the classroom**, failure to do so will result in confiscation.
- Students are not permitted to access or use mobile devices on school property, inclusive of after school events/study and training, unless directed by a teacher. Failure to comply with this policy will result in the confiscation of the device.
- Students wishing to contact their parents may do so from the phone in the school office. They should not use their own mobile phone for this purpose while on school property.
- In certain classes as pre-arranged by the class teacher, specific teaching and learning or research activities may require access to a personal mobile device. Such access and usage will take place under the clear, focused guidance and supervision of the teacher with defined learning intentions and once that activity is completed students will be required to turn their mobile devices off and stow them safely in their bags. Such access is limited to that specific activity and is governed by the St. Joseph’s Patrician College’s AUP. It is the student’s responsibility to ensure that the phone does not disrupt any subsequent classes.
- The School does not permit the streaming of music through mobile devices at any time on school property.
- In certain classes as pre-arranged by the class teacher, specific teaching and learning or research activities may require access to Ear-phones / ear-buds. This is the only circumstance where they can be used on school property. Students should store ear-phones and/or ear-buds away in school bags and/or school-jacket pockets

once on school premises. Failure to do so will result in the confiscation of these devices.

- Students found not complying with the above will face having their mobile phone confiscated and the offence noted on Compass. Confiscated mobile devices will be held securely on site and parents will be required to come to the school and sign for the return of a mobile phone. This return-service will be available from the school office only.
- Any mobile device not claimed within three months will be disposed of.

• 1st Offence	• Returned at end of day.	• Collected by student
• 2nd Offence	• Returned after 3 school days	• Collected by Parent / Guardian after 3 days. (At end of school day)
• 3 Offence	• Returned after 1 school week (5 days)	• Collected by Parent / Guardian after 5 days. (At end of school day)

- Parents wishing to contact their son/daughter are required to do so by contacting the school office on 091- 565980.
- Photographs cannot be taken, nor can recordings (audio or visual) be made, of a member of the school community without his/her expressed permission. Using phones or any other recording devices to record a person without appropriate authorisation, will be considered a serious breach of the School's Code of Responsibility and Behaviour, up to and including Step 9 of our Code.
- School staff will act uniformly in accordance with this policy. Refusal to hand a mobile device over to a staff member, on instruction, will be dealt with through the St. Joseph's Patrician College Code of Responsibility and Behaviour.
- It should be noted that it is a criminal offence to use a mobile device to menace, harass or offend another person. As such, the school may consider it appropriate to involve An Garda Síochána in such incidents.

Procedures to follow if policy breach is identified:

- If addressed by a staff member regarding using/accessing a mobile device the student may turn off his/her phone (the SIM is not permitted to be removed from a confiscated device)

- The device is handed to the teacher

- The device is enveloped with the name of student the date/time and the staff member's name clearly recorded on the envelope

- The device is handed into reception and stored securely for collection

- Teachers record this event on Compass.

- A Parent/Guardian is required to come to the school to recover the mobile device from reception and sign for the collection of the device.

Social Media and Mobile Phone Use on Approved School Trips / Tours / Extra Curricular (School Business) AUTHORISED SCHOOL BUSINESS (e.g. games, field trips, etc.):

(a) Photographs cannot be taken, nor can recordings (audio or visual) be made, of a member of the school community without his/her expressed permission. Using phones or any other recording devices to record a person without appropriate authorisation, will be considered a serious breach of the School's Code of Behaviour.

No photographs of, or recordings (audio or visual) of, or comments about a member of the school community can be uploaded to the Internet without his/her expressed permission and the permission of the school Principal/Deputy Principal.

(b) Students will observe positive 'netiquette' (i.e. etiquette on the Internet) in their representation of and comments on members of the school community and about the school itself (refer to the AUP)

(c) Students will not upload, download, send or forward any material on the Internet that is obscene, defamatory or intended to annoy or harass a member of the school community.

(d) Instances where the Internet is used to insult, offend, slander, defame, harass or bully a member of the school community by another member of the school community is a serious offence and will be treated accordingly. Any student who uses the Internet as a vehicle to insult, offend, harass or bully another student or staff member will be deemed to have committed a serious breach of the School's Code of Responsibility and Behaviour and the school will have recourse to the range of sanctions available. The school may consider it appropriate to involve the Gardaí in such instances.

Serious breaches of the School's Code of Responsibility and Behaviour will be dealt with by the appropriate Year Head, and/or the Deputy Principal/Principal and may be reported to the Board of Management.

It is intended a summary of this Policy will be in the Student Journal **(Appendix A**). Parents/Guardians and students will be asked to read and sign their acceptance each year.

Real-time teaching and learning:

Teachers and pupils should be using the school's contracted service providers **Microsoft office 365** for school related communications.

Ad-hoc use of apps or services by individual teachers and students is discouraged.

- Where video-conferencing services are being used for school purposes, the school will have assessed these platforms and services providers for privacy and security. The only platforms permitted as a video conferencing service are **Microsoft Team or Cisco Webex**.

- Provision of clear, understandable, and up-to-date organisational guidelines will ensure that teachers know what rules to follow and steps to take to minimise risks (e.g. data protection, child safeguarding, teacher safety etc).

- All members of the school community (students, teachers, parents) should understand that all the standard school policies are still applicable in this remote teaching scenario (e.g. Code of Responsibility and Behaviour, Acceptable Use Policy, Anti-Bullying Policy, Social Media Policy etc.)

- The school will ensure that teachers use work accounts, email addresses, phone numbers, etc., where possible, for school-related video-conferencing.

- Teachers should familiarise themselves with the controls available within the service and how to use these controls to protect their security, data, and communications. (Most of the service providers have published help-pages and/or video tutorials that explain how this should be done).

- St Joseph’s Patrician College will implement, and require teachers to implement, appropriate security and access controls. A key issue to determine is how access to the online classroom will be controlled. The teacher will control who joins the online class group.

- All users (students and teachers) limit their data sharing. Maintaining a strong focus on the learning content is likely to minimise the sharing of personal data.

- St Joseph’s Patrician College will consider the circumstances (if any) in which the school or teachers will allow student sharing of video/audio stream. It is nearly always best practice that students join with camera/microphone disabled (by the host).

- The serious consequences for anyone acting to record or screen shot an online lesson should be emphasised (not least the fact that such activity is likely to be unlawful where personal data is captured)

<u>The School and teachers should:</u>

- Keep the application updated at all times

- Prioritise using the Web Browser over Desktop or mobile application to access your web conferencing application

- Enable Multi-Factor Authentication (MFA) on your Web-Conferencing account

- Use a password or PIN function where available to enter meetings and only share it with those scheduled to attend the meeting

- Send passwords or PIN via out-of-band means e.g. text or Signal message. Use of the meeting ID function is preferable to sharing a link

- When scheduling a meeting avail of "Waiting Room" or "Green Room" function

- Make sure to enable features that alert of newly joined participants - audible tone

- The host should restrict who is allowed to use their camera and microphone

- Minimise the use of the chat and file sharing functions or disable entirely if not required

- Do not give control of your screen unless you know and can verify the individual you are passing control (Present in same room)
- Select "Lock Meeting" function or similar once all expected guests have joined the meeting
- Before starting a meeting, make sure to check who exactly is on the call from the Participants menu. Participants should join with their name visible.
- Consider making registration a requirement
- Do not record meetings unless it is strictly necessary.

The school will inform parents and students of the importance of correct procedures, customs and practices during remote teaching.

Operating transparency is both a legal requirement and also an important means of mitigating risk. The school approach this by communicating clearly with parents and students in advance (**Appendix B**)

Cyber Bulling:

When using the internet pupils, parents and staff are expected to treat others with respect at all times. Engaging in online activities with the intention to harm, harass, or embarrass another pupil or member of staff is an unacceptable and absolutely prohibited behaviour, with serious consequences and sanctions for those involved. Measures are taken by St. Joseph’s Patrician College to ensure that staff and pupils are aware that bullying is defined as unwanted negative behaviour, verbal, psychological or physical, conducted by an individual or group against another person (or persons) and which is repeated over time. This definition includes cyber-bullying. Isolated or once-off incidents of intentional negative behaviour, including a once-off offensive or hurtful text message or other private messaging, do not fall within the definition of bullying and may be dealt with, as appropriate, in accordance with the School’s Code of Behaviour. The prevention of cyber bullying is an integral part of the Anti-Bullying Policy of our school.

Legislation:

The school will provide information on the following legislation relating to use of the Internet which teachers, students and parents should familiarise themselves with these acts

Legislation pertaining to use of the Internet includes but is not limited to

- Data Protection Act 1988 (and Amendment Act 2003) and GDPR 2018.
- http://www.dataprotection.ie/
- http://www.irishstatutebook.ie/1988/en/act/pub/0025/index.html
- http://www.irishstatutebook.ie/2003/en/act/pub/0006/index.html
- Child Trafficking and Pornography Act 1998
- http://www.irishstatutebook.ie/1998/en/act/pub/0022/index.html
- Interception Act 1993
- http://www.irishstatutebook.ie/1993/en/act/pub/0010/print.html
- Video Recordings Act 1989
- http://www.irishstatutebook.ie/1989/en/act/pub/0022/index.html

Sanctions:

Misuse of the Internet will result in disciplinary action, including verbal and/or written warnings, withdrawal of access privileges, suspension and, in extreme cases, expulsion. The St Joseph's Patrician College also reserves the right to report any illegal activities to the appropriate authorities.

SUPPORT STRUCTURES:

Where appropriate, the school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet.

This policy has been made available to the Parents' Council, Student Council and Staff. It is available to all partners on request.

DESIGNATED LIAISON PERSON (DLP) John Madden (Principal) DEPUTY LIAISON PERSON Seamus Cahalan (March 2021-March 2022)

The Board of Management ratified this policy on the:	DATE: 5th November 2021.
	Signed:
Myles McHugh Chairperson	Myles McHugh.
John Madden Secretary of the BOM	John Madden
Date of next review:	As required

Appendix A

For Inclusion in The Student Journal 2021-2022

MOBILE DEVICE POLICY

This policy in relation to mobile phones is to ensure:

1. That the teaching and learning activities are not impeded by mobile devices and incidents involving mobile devices

2. That students are not late for class

3. That students are concentrating exclusively in class on active learning

4. That text/video bullying and intimidation is prevented.

5. That individual privacy and personal safety are not undermined in the school community

6. That learning activities involving mobile devices are pre-arranged, managed and supervised by class teachers.

This Policy applies to the entire school campus which includes the school buildings, environs and **all school related activities** that occur on-site and off-site in the name of the school.

- If mobile phones are brought to school, the school accepts no responsibility for replacing lost, stolen or damaged mobile phones. The safety and security of mobile phones is wholly a matter for students / parents.
- If brought to school mobile phones must be stored throughout the day in students school bag /secured in student locker so as not to disrupt learning and teaching in class. **It is the student's responsibility to make sure their phone does not disturb the classroom**, failure to do so will result in confiscation
- Students are not permitted to access or use mobile devices at any time, unless they are directed by a teacher. Such access and usage will take place under the clear, focused guidance and supervision of the teacher with defined learning intentions and once that activity is completed students will be required to turn their mobile devices off and stow them safely. Failure to comply with this policy will result in the confiscation of the device.

- The School does not permit the streaming of music through mobile devices at any time in the school day.
- Ear-phones / ear-buds /speakers are not to be used nor are they to be visible during the school day.
- Students wishing to contact their parents may do so from the phone in the school office. They should not use their own mobile phone for this purpose while on school property.
- Parents wishing to contact their son are required to do so by making contact with the school office on 091 565980. Parents will be contacted as required through the school office.
- Confiscated mobile devices will be held securely on site and parents will be required to come to the school and sign for the return of a mobile phone.
-

• 1st Offence	• Returned at end of day.	• Collected by student
• 2nd Offence	• Returned after 3 school days	• Collected by Parent / Guardian after 3 days. (At end of school day)
• 3 Offence	• Returned after 1 school week (5 days)	• Collected by Parent / Guardian after 5 days. (At end of school day)

- Any mobile device not claimed within three months will be disposed of.
- School staff will act uniformly in accordance with this policy. Refusal to hand a mobile device over to a staff member, on instruction, will be dealt with through the St. Joseph’s Patrician College Code of Responsibility Behaviour.
- It should be noted that it is a criminal offence to use a mobile device to menace, harass or offend another person. As such, the school may consider it appropriate to involve the Gardai in such incidents.

Appendix B

(Sample text of letter/ communication to parents below).

Dear Parent/Guardian

As part of its delivery of remote learning, the school is organising a series of virtual classroom events to allow teachers and students to interact in real time using the **Microsoft Team or Cisco Webex** video conferencing platform. Teachers will communicate the details and scheduled times to students by email and their school email account will also be used to control access to each virtual lesson Care is needed to ensure the online security of everyone involved.

Students are reminded that all of the school's policies, notably the Code of Responsibility and Behaviour and the Acceptable Use Policy, apply during these online lessons. When students join a virtual lesson their device cameras and microphones are off by default (this setting is controlled by the teacher). However, as the virtual classroom provides an opportunity for participation, teachers may encourage some audio and/or video interaction with students. Students are being advised of best practice around this participation e.g. quiet location, proper attire, no personal information visible in background (bedrooms etc best avoided) etc.

No live recording will be done using the MS Teams or Cisco Webex videoconferencing platform. This is to respect the personal data of all, both teachers and students, who participate in each virtual lesson. All are reminded that no recording (or screen photograph) of any part of the video lesson should be made by any other means. The recording and onwards sharing of personal data would be unlawful as well as a contravention of the school's policies.

The school appreciates your support to ensure that best learning outcomes are achieved while also respecting everybody's privacy at home. If at any stage you have any concerns or wish to provide any feedback then please do not hesitate to contact the school.

Yours Sincerely.

Appendix C

Blended learning Approach:

We have devised a new Remote Learning Policy to reflect the changing circumstances brought about by Covid-19 and the significant increase in the use of technology to continue learning. This policy does not introduce any new concepts, rather, it specifically outlines the various applications used for the delivery of online classes remotely.

This section sets out the policy of the school in respect of use of technology for distance or remote teaching and learning if we are directed to give home instruction due to Coronavirus or any other reason, hereafter referred to as "Remote/Distance eLearning" – it operates in addition to our existing Acceptable Use Policy (AUP).

In the event of a blended learning or full remote teaching being required our normal school timetable will apply.

Scope of this Policy

This policy covers any aspect of student distance/remote eLearning as used by school staff.

In all cases students must use their school Teams account to log in. Students are not to use any other account under any circumstances for the purposes of Remote/Distance eLearning within St. Joseph's Patrician College.

The list of applications that will be used for distance learning will primarily be:

□ Microsoft Teams

□ Microsoft Outlook Email

□ Cisco Webex for live online classes

There may be some additional applications that teachers may use, and the teacher will provide the student with the information required to access them through google classroom. This must, in all cases, use a school account as the login.

If a student is having difficulty with accessing a digital device the school will endeavour to provide that student with the loan of a device were possible. Everyone’s Responsibilities while partaking in remote Learning

For staff and teachers:

□ Teachers have overall control of the online interaction of their class

□ Disruptive students will be removed in order to allow those who wish to partake a fair chance to do so. Repeatedly disruptive students may receive a temporary ban from all online access.

□ Teachers will do their utmost to be available at the identified time on their timetable – this may be via a Teams live video, through Teams or by email.

For students:

□ You are to communicate through your school @bish account only. The use of any other account or e-mail address is completely prohibited

□ Do not engage in communications with any account other than a school account unless directed to do so by your class teacher and report any such activity to your teacher or the Senior Management Team

□ You must always be civil and respectful to your teachers and fellow students

· You are not to record or forward any content within a digital learning group – such as worksheets, exam papers, answers, solutions, videos, notes or Teams links – to anyone else without the permission of the creator of that content

□ You understand that all your online activity is recorded. This includes anything you send or say via e-mail and Teams , and whether you are checking regularly for assigned work and engaging in online lessons to the best of your ability

. □ You must be available to attend your timetable classes via Teams , etc as expected during the school day.

For parents:

□ You should ensure that your son is checking in regularly for live lessons and assigned work.

□ Where live classes are being run you should ensure your son is in an area of the house that is quiet and free from distractions, if possible. Please be mindful of Child Protection Guidelines, for example, if possible bedrooms should not be used for live classes

□ Live online classes should be viewed by your son/ daughter only. Live Online Classes Teachers may deliver some of the Remote eLearning "live" using Teams or other digital platforms. This will use varying combinations of audio, video, virtual whiteboards and screencasts.

In the use of Teams:

□ Students must always follow the direction of their teacher just as in the classroom

□ Students are not to turn on their video at any time unless directed to do so by the teacher.

□ Students are not to turn on their microphone unless the teacher invites them to do so. In any case, all microphones should be on mute when a person is not speaking to avoid distracting background noise being broadcast to everyone.

□ A Team link is intended for the student only. The teacher will decide who should receive the link. Do not forward any link to anyone else.

□ Team sessions may be recorded, and these recordings may be made available by the teacher to the class to watch back again later. This recording includes any video, screenshares, whiteboards and audio from the class.

□ Only the teacher is allowed record a session. No-one else is permitted to record

Appendix D

Remote Parent Teacher Meetings:

‘School Cloud’ trial for PT Meetings for 2nd year on November 11th:

Proposed Appendix D to AUP Policy:

Acceptable User Policy (AUP) relevant to students, staff and parents :

Collecting and Processing Data::

As per our GDPR Data Protection policy available on bish.ie.

There will be no change to the way we collect or the way we process data.

- We are relying on the fact that the data processing is necessary for compliance with a legal obligation or a task carried out in the public interest i.e. processing activities that stem from the school’s obligations to deliver public education.

Processing Activities Undertaken by the School:

We have collected this data previously and it is noted in our GDPR policy. This policy sets out the purposes for which the school collects and uses personal data for each of the various categories of data held (student, staff, parent, etc).

7.5.3

- **Student Records:** The purposes for processing student personal data include the following:
- To provide them with appropriate education and support.
- To monitor their academic progress.
- To comply with our legal obligations as an education body.

7.5.4

Staff Records:

- We use staff personal data for purposes including:
- To coordinate, …… and organise educational programmes.

In advance of retaining this service provider the following checks have occurred:

- Due diligence of service providers (data processors) prior to any service being retained.
- Adequate assurances of GDPR compliance have been obtained.
- End-User Privacy Notice is in place
- GDPR policy in place.
- Security and data Protection details in place.
- Meetings are not recorded as they're encrypted end to end for users.

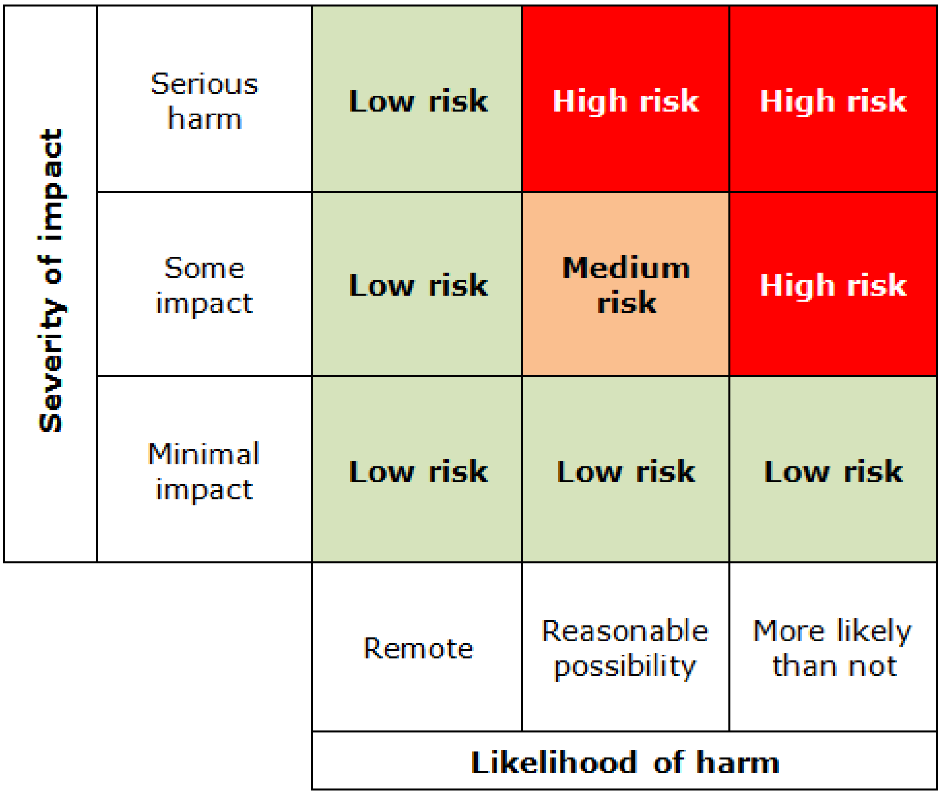
Is a Data Protection Impact Assessment (DPIA) Required? :

- See Screening questionnaire completed (Appendix E) on proposed 'School Cloud' Trial. November 2021.

It is our opinion that a DPIA is not required at there is no 'High Risk' to other people's personal information.

The following Risk assessment was also conducted:

The following matrix was used to assess Risk:



Severity of impact	Serious harm	Low risk	High risk	High risk
	Some impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

Risk to	**Nature of Risk**	**High**	**Medium**	**Low**	**Mitigation**
Teachers	*Over-sharing of personal data i.e. where it is either unnecessary or inappropriate (e.g. camera images from teachers' homes that may cause offence.*			X	There is a blur background feature in the software.
	Unlawful data capture from the live stream and subsequent misuse by students (e.g. screen shots or photographs of teachers being shared onwards via social media);			X	Expectations shared with parents in advance of the meeting.
	Unlawful access to the live stream by third parties (e.g. security gaps allowing strangers to join classes or share inappropriate content).				Security feature built into software that will not allow this to happen. Each individual meeting is a standalone event.
	Types of Data Being processed (Title, name, surname, email address, 4 digit Compass code)			X	Not sensitive data.
	Clarity for teachers around operational measures.			X	Instruction video to be shared with staff and parents in advance of the meeting.
Parents					
	Share school expectation with parents			X	Communicate expectations in advance of meeting
	Types of Data Being processed (Title,			X	Not sensitive data.

	name, surname, email address)				
Pupils	*Types of Data Being processed (name, surname, Year, class and Compass user ID, Date of birth,)*			X	Not sensitive data.
Class	*Types of Data Being processed (group name eg 2D, teacher and student)*			X	Not sensitive data.
IT	Platform Secure			X	Consultation with other schools who have used this and similar platforms.
	Track record in providing secure service to schools.			X	

Risk Assessment carried out by:

PJ Folan,

Seamus Cahalan,

John Madden.

- Following advice from Data Protection Advisor JMB.
- Data Protection Commission website also consulted.
- Video-conferencing facilities can be used where available, and where parents/guardians and teachers have appropriate digital access. Recommended by DES and approved by ASTI.

The Board of Management ratified this appendix to the AUP policy on :	DATE: November 5th 2021.
	Signed:
Myles McHugh Chairperson	Myles McHugh.
John Madden Secretary of the BOM	John Madden
Date of next review:	As required

Appendix E

Screening Questions for a Data Protection Impact Assessment for School Cloud Trial November 2021.

Screening Questions

Note: Each screening question should be answered, and you should add any additional, relevant question(s) dependant on the risk and/or processing operation(s) you are assessing. These screening questions will help you to identify if a DPIA is required and provide valuable insight into the processing operation risks and areas to focus on.

Screening Question	Yes	No	N/A	Notes
Does the processing require systematic and/or extensive evaluation *(via automated means*) of personal aspects of an individual(s)?		√		
Will decisions be based on such evaluations that are likely to produce legal effects, or equivalent effects concerning the individual(s)		√		
Is the processing on a large scale and/or does it involve special categories of data (sensitive data)?		√		
Is the processing on a large scale		√		
Does the processing involve systematic monitoring of a publicly accessible area on a large scale? (i.e. CCTV)		√		
Will the project involve the collection of new information about individuals?		√		
Will the project compel individuals to provide new information about themselves?		√		
Are you using information about individuals for a purpose it is not currently		√		

used for, or in a way it is not currently used?				
Screening Question	**Yes**	**No**	**N/A**	**Notes**
Is the information about individuals likely to raise high risk privacy concerns or expectations?		√		
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information or a third-party without adequate safeguards in place?	√			Protected under the *'School Cloud'* Security platform
Does the processing involve the use of new technology or systems which might be perceived as being privacy intrusive?		√		New Software Only
Could the processing result in decisions being made or action being taking against individual(s), in ways that could have a significant impact on them?		√		
Will the project require you to contact individuals in ways which they may find intrusive?	√			Risk Assessment defines as ***Low Risk***
Will any of the processing activities make it difficult for the data subject(s) to exercise their rights?		√		
Will the operation involve processing considerable amounts of personal data at regional, national or supranational level, which could affect many data subjects?		√		
Will the processing involve individuals who are considered 'vulnerable'?		√		
Does the processing operation involve any significant risk of the personal information being leaked or accessed externally?		√		