SHS Acceptable Usage Policy

All students and parents are required to carefully read this document and sign their acceptance of the Policy. Use of the IT is dependent on the Policy being signed and returned to the School.

1. **Introduction:** This Acceptable Usage Policy ("**AUP**") sets out the School's requirements for students' use of and access to IT in School.

IT	All information technology resources, systems, internet, all tools within the Microsoft Office 365 environment (including Word, Email/outlook, Teams etc), school networks, other network resources, devices (including Microsoft Surface Pro/Go, mobile phone, laptop, tablet, desktop, and all other internet-enabled devices etc), hardware, software, apps, and other IT facilities (regardless of whether the IT is managed by the School or by a third party or data processor on behalf of the School).
Device	Any mobile phone, laptop, tablet device, desktop computer, hard-drive, other storage device, or other internet-enabled device (including any internet-enabled wearable devices like Apple Watches etc), (regardless of whether the Device is owned by the School, managed by the School, or was purchased by a student/their parent or guardian but brought to the School and on or from which a student can access certain School IT systems/networks).
Access	Means any form of access to School IT whether on-site (physically from the School premises) or off-site by logging in remotely.
Standards	The standards of conduct stipulated in this AUP
Monitoring	All forms of monitoring undertaken by School staff and School systems during school hours (8.45am to 3:15pm) in either manual monitoring form (ie student required to hand over

	Device) or in system monitoring format (SENSO software – see Appendix 1 Fair Processing Notice) to ensure each Student is complying with this AUP. Student screens and web-search activity and all other Device activity is monitored during class time to ensure Students are on-task with their classwork.

The AUP also explains how Standards are monitored/observed to prevent or detect misuse or harmful activity (eg. device management, anti-virus scanning, SENSO software), how complementary school policies interact with this AUP to address any misuse of IT (eg. Anti-Bullying Policy etc), when and in what circumstances Consequences will be applied (see section 6 of this AUP), what procedures will be followed, when and in what circumstances parents are notified, and when and in what circumstances reports are made to An Garda Síochána and/or TUSLA (Child and Family Agency) by the School.

2. **Rationale:** IT resources at Sacred Heart School (SHS) are provided/supported consistent with the educational mission of the School. Sacred Heart School hopes that the privilege of using IT will deliver learning and development opportunities for students. The School's goal in utilising IT (including the Surface Pro/Go) is to promote educational excellence by facilitating resource sharing, innovation, research, creativity, communication, increased productivity, and mobile learning. The School fosters a supportive and safe environment for Students to learn. The School also has a duty of care to protect all students, and to protect IT resources against misuse.

3. **Aim of our Acceptable User Policy:** The aim of this AUP is to ensure that students will benefit from learning opportunities offered by the school's IT in a safe and effective manner. Use of the School's IT during class-time, including the privilege to use a Device in the classroom to enhance the learning experience, is considered a school resource and privilege. The privilege can be withdrawn if the student does not comply with acceptance standards of behaviour and/or otherwise breaches this AUP. This aim of this AUP is to set out:

(a) **Clear Standards**: Specifying the Standards of behaviour all students are expected to demonstrate, and reminding students of the relevant policies applicable to support acceptable standards of behaviour from students (cross-reference with the School's Code of Behaviour, Anti-Bullying Policy, Child Safeguarding Statement, Social Media Policy etc). All examples used in this AUP are for illustrative purposes only, and are not intended to be exhaustive. The School will take all reasonable measures to uphold acceptable standards of behaviour, take action against irresponsible or unacceptable behaviour, and to protect the school from legal liability including from student misuse or abuse of IT. The Standards outlined in this AUP shall be interpreted broadly to support the School upholding acceptable standards and to protect its legitimate interests.

(b) **Consequences**: The measures that will be taken when a student falls short of what is expected (a ladder of consequences depending on the seriousness of the misuse or breach). This includes alerting students/parents/guardians to instances where the School may notify An Garda Síochána (eg. criminal damage, hacking, disseminating illegal images, accessing pornography, hate-speech, harassment, threats to harm, or accessing or distributing harmful materials etc) and notify TUSLA (Child and Family Agency) (eg. disclosures of abuse, harm or risk of harm to self, harm or risk of harm to others, welfare concerns etc). See further the Consequences section at Section 6 of this AUP.

(c) **Procedures**: the procedures that will be followed by the School in response to breaches of this AUP by a student(s) (ie on-ramp to the Code of Behaviour that could lead to suspension and/or expulsion).

4. **Clear Standards:** Use of IT in school and in class is a <u>privilege</u> and can be withdrawn if a student falls short in the behavioural expectations consistent with all school rules and policies, including but not limited to those stated in the Code of Behaviour. This AUP is to make all users aware of their personal responsibilities associated with efficient, ethical, and lawful use of IT. Any misuse or breach of the Standards shall result in Consequences (see section 6 of this AUP). If a person violates any term of this AUP, privileges may be terminated (or withdrawn for a period), access to the school's IT may be denied (in whole or in part), the appropriate disciplinary action shall be applied (School Code of Behaviour which can lead to disciplinary action up to and including suspension and/or expulsion for a student) and in appropriate cases the matter may be reported to An Garda Síochána and/or TUSLA. All examples given in this AUP are for illustrative purposes only, and are not

intended to be exhaustive. The Standards applicable in this AUP include the following:

4.1 **I will behave ethically and responsibly:**

(a) Students shall use IT in full compliance with this AUP.

(b) Students must comply with the School's Code of Behaviour and Anti-Bulling Policy.

(c) Students' use of IT must be responsible, ethical, and legal.

(d) Students must treat others with respect at all times.

(e) Students shall not engage in any unacceptable, offensive, or harmful behaviour, or engage in any activity that could bring the School into disrepute.

(f) Do not use offensive or obscene or rude language or send, post, publish or circulate anything offensive, obscene, or rude (including in your messages or emails to other people).

4.2 **I will never leave the Device unattended. I will know where my Device is at all times.**

(a) If a device is found unattended, it should be given to the nearest member of staff. Also, students are advised not to leave their device unattended in a vehicle.

(b) Have a lock for your locker. It must be always locked. Keys to lockers should be worn on lanyard or kept in a safe place. Devices are to be left in lockers when students are on School tours, trips and activities (or left at home if the Student will not be in School).

(c) Take care not to leave their Device on table edges or in any position where damage could occur.

(d) Students should set their Devices to lock automatically after a few minutes of non-use

(e) Keep the Device in a secure location when not in school.

4.3 **I will never lend my Device to someone else**

(a) Pupils should not share/reveal passwords or log-in details with other students.

(b) Do not provide your personal information or log-in credentials to anyone over the Internet.

(c) access to School IT is not transferable or permitted to be used by any person, people or groups outside the school.

4.4 **I will respect that IT is a privilege for educational use in class and for use by SHS Students only:**

(a) Teachers shall provide clear guidance to students during class so that they can understand what is permitted and what is prohibited. Teachers will support students in understanding that Devices are for educational use only.

(b) Devices are a privilege for educational use during class-time only. Students shall not use their Device in school corridors, or on school grounds outside of class time, and shall not use a Device during lunchtime or break-time: this is “Screen free time”. Modification to “screen-free time” is only with a Teacher’s prior permission.

(c) There will be “Screen Down” time in many, if not all, classes during the day. Students must follow all instructions of teachers in class regarding use of or putting away of Devices.

(d) Use of Devices is a privilege, and should be used for classwork only. Students are not allowed to use any App in school which is unrelated to class work.

(e) Students shall use IT for their own educational use only. Students must not share log-in credentials or passwords with any other person.

(f) Use IT for the period they are a student only; access to School IT ceases concurrently with a student ceasing to be enrolled in the school.

(g) Before arrival to school, and at the start of each class, each student shall ensure that all Apps are closed.

(h) Ensure your eBooks are installed and working properly. Any issues or faults should be reported to the Year Head/Principal.

(i) Usernames and passwords for eBooks should be retained in the note's app of each pupil's device. Username and password for email should be noted in a secure location that other students do not have access to.

(j) Teachers are authorised to monitor the most recently used apps, most recently visited websites, most recent online activity etc. on a student's Device to ascertain that the student is “on task” and properly completing the class-work without distraction. If a teacher engages in monitoring for this purpose, the Student shall not object or cause an obstruction to the monitoring.

(k) Use of or access to any social networking or social media app is strictly forbidden during school time. This may result in suspension.

4.5**I will take good care of my Device and be responsible for my use of my Device. I will charge my Device battery every night.**

(a) Arrive to school each day with a fully charged Device; disciplinary action will be taken if this is not observed. If a Device is left at home or is not fully charged, the Student remains fully responsible for completing all schoolwork as if they had use of/access to their Device.

(b) In the event of any disciplinary action leading to the withdrawal of a Device or restriction of privileges to access IT, the completion of all class work remains the responsibility of the pupil.

(c) Malfunctions of Device or technical issues are not acceptable excuses for failing to complete schoolwork, unless there is no other reasonable means of completion.

(d) The School will try its best to assist students to resolve any technical or other issues.

(e) Have a protective case for their Device. Do not remove the device from any protective case.

(f) Keep the Device clean. For example, do not eat or drink while using the device.

(g) Do not subject the device to extreme heat or cold.

4.6 **I will not disassemble any part of my Device, personally attempt any IT repairs, or attempt to undermine SHS IT security**

(a) Do not do anything to the Device (download software or otherwise) that will permanently alter it in any way.

(b) Do not remove any serial numbers, identification or school labels placed on the Device.

(c) Report any problems, issues, damage, or theft of any Device immediately to either the year head or principal, deputy principal or Year Head.

(d) The School will try its best to assist students to resolve any issues. The School will make every effort to resolve reported issues relating to ownership, possession, theft, or misuse of the Device.

(e) On occasion, circumstances may arise where a Device may need to be repaired in-house. In this case you may be asked to share your password with one of the members of the Staff or Student Digital Support Team to ensure your tablet is fixed as quickly as possible. We suggest you change your password after the fix is installed, to keep your passwords secure.

(f) Report any issue and /or interference created by or a as result of any act or activity by any other students because of device possession, use or ownership. A student is obliged to report any damage or interference that may have occurred to their Device during the school day ON THE DAY THE INTERFERENCE/DAMAGE OCCURED. Otherwise, school management may presume that the damage and/or interference took place outside of school time.

(g) The school is not responsible for any loss or damage to students' property.

(h) Students must observe all terms and conditions for use of the Microsoft 365 environment.

(i) Do not install any software on to the Device or into the School IT environment without prior written approval from a Year Head.

(j) Students must not undermine, disable, or turn off any security feature or protective feature (including but not limited to antivirus, firewall, web-filter etc).

(k) Students shall not attempt to subvert or bypass or disable any security feature installed on any Device or any form of web-filter or firewall applied by School IT.

(l) Students must not introduce anything harmful in to the School IT system, such as a virus or spyware or malware.

(m) No student shall attempt to "jail break[1]" their Device, or otherwise attempt to bypass any security feature (including the

[1] Any attempt to remove or bypass restrictions or safeguards imposed on the Device or IT.

SHS webfilter or firewall) through using a VPN[2] or web proxy or anonymous server (eg TOR) or by using SSH tunnelling or otherwise.

(n) Do not hack or attempt to hack the School IT (or any network or part thereof) or otherwise attempt to access, interfere, or intercept the transmission of any data on the School IT. Hacking is a criminal offence, and will lead to the Gardaí being involved. Any hacking attempt shall be reported to An Garda Síochána per Criminal Justice (Offences Relating to Information Systems) Act 2017 and Criminal Justice Act 2011.

(o) If a Student suspects their Device or any IT may have a virus or that spyware has been installed, immediately power down and close your Device, and contact a Teacher immediately.

4.7 **I will be responsible for my health and mental wellbeing while using the Device:**

(a) Avoid extended use of the Device while resting directly on your lap. The bottom of the Device can generate significant heat.

(b) Take frequent breaks when using the Device, do not use the Device uninterrupted for long periods of time. Look away from the device approximately every fifteen minutes to minimise neck or eye-strain.

(c) Students are advised not to use their device during their lunch breaks.

(d) Talk to a teacher or Year-Head if there is anything worrying you relating to what you have seen or accessed via the Device, or if anything has made you feel uncomfortable.

(e) Talk to a teacher or Year-Head if anyone is cyber-bullying you.

(f) Talk to a teacher or Year-Head if anyone sends you an image you are uncomfortable about, or takes an image of you that you did not consent to.

(g) Refrain from posting your personal information online. Take care when talking to people online, and try to exercise caution about what you share about yourself.

[2] Virtual Private Network.

(h) Do not use your Device or School IT to sext[3] another person, or to create intimate content, or make or send self-generated images (nudes, nude-selfies etc), or to share intimate images of any other person(s).

(i) Do not use your Device of School IT to take or send or share images of another person that could cause that other person distress, embarrassment, humiliation, or for the purpose of denigrating that person.

(j) Talk to your teacher or Year Head (or ask your Parent/Guardian to contact a teacher or Year Head) if you are worried or distressed or uncomfortable about anything. The School can provide support if you are experiencing cyber-bullying, or if you are experiencing worries about something someone has sent you, or something you have sent another person (eg. self-generated images or sexting) and someone has shared it with others without your consent (eg. revenge porn).

4.8 **I will only photograph people with their permission. I will only use the camera or the microphone when my teacher tells me to.**

(a) Students must be respectful of their peers, and must observe informed Consent. Students may not photograph any other person, without that other person's informed consent.

(b) Use of the camera and/or microphone is strictly prohibited unless prior permission is granted in advance by a Teacher.

(c) Users must use good judgment when using the camera. Regardless of your intention, do not take a photograph that could cause upset, offence, harm, distress, embarrassment, or humiliation to another person.

(d) Images of other people may only be made with the permission/informed consent of those in the photograph.

(e) Taking, posting, or uploading any image(s)/video(s)/recording(s) whether audio or visual of any Teacher or SHS staff to the Internet or to any social media platform (whether to a closed group or otherwise) or to any other public forum is strictly forbidden, without the express permission of that Teacher /member of Staff.

[3] See PDST resource at footnote 5, meaning a sexually explicit message.

4.9 **I will not use my device in toilets or dressing rooms, and I will respect other people's privacy**

(a) People have a reasonable expectation to privacy in certain areas. Students must respect other people's privacy.

(b) Any use of camera in toilets or changing rooms, or other areas where a person has a reasonable expectation of privacy will be treated as a serious violation of this AUP, regardless of whether or not you intended to cause distress or breach another person's privacy.

(c) Respect other people's privacy. This may include you not sharing or re-posting the contents of messages other people have sent you if doing so could result in them being humiliated or intimidated by others. However, if you are worried about anything someone has said to you or sent to you (eg. cyberbullying, or online grooming, or someone has sent you sexually intimate images etc) or anything has made you feel uncomfortable or unsafe (eg. hate speech, threats, racism, etc) please speak to your teacher or Year Head, or ask your parent/guardian to contact your teacher or Year Head so that you can be supported.

4.10 **I will not use my Device or School IT for financial or commercial gain.**

(a) Students are not permitted to use the Device to run a business, undertake any commercial activities, offer services or take payment for services.

(b) Students are prohibited from using a Device or School IT to access betting or gambling or websites.

4.11 **I will not use my Device to bully, intimidate, harass, humiliate, hurt, defame, or abuse others**

(a) At no time is it ever acceptable to use any IT or Device for the purpose of bullying, intimidating, harassing, humiliating, or hurting another person or group of people.

(b) Do not post or share or distribute anything that could harm another person.

(c) Do not post or share or distribute anything that is false or defamatory (ie damaging to another person's reputation).

(d) Do not harass or beset another person (ie engage in unwanted conduct, or unwanted repeated contact, including anything that violates their privacy or could be intimidating or humiliating).

(e) Students are prohibited from writing, publishing, posting, disseminating, sharing, circulating, uploading or creating inappropriate, defamatory, inaccurate, abusive, intimidating, harassing, or racist material on their Device or using IT.

(f) Inappropriate media (media in breach of copyright or intellectual property, media containing inappropriate or offensive language or imagery) shall not be used as a screensaver or background photo.

(g) Students are not permitted to do any thing or take any action that could bring the School into disrepute;

(h) Students may be requested at any stage to provide their Device for inspection to any member of the school staff.

(i) if a student is suspected or reported to be cyberbullying, cyberstalking, engaging in any form of harassment using IT, or engaging in any form of illegal activity etc, the matter will be reported to An Garda Síochána and TUSLA, who have the necessary skill-set to investigate such incident.

4.12 **I will not use School IT to access or search for or post or share illegal or harmful content, or to conduct any illegal activity, or otherwise break the law**

(a) Students must not create, download, store, make, take, record, post, share, publish, distribute, or threaten to distribute/public/share/send harmful or distressing, (eg. animal cruelty content, content showing injury to others).

(b) Students shall not engage in any harassment, defamation, or hate-speech[4] using the IT or their Device.

(c) Students must not create, download, store, make, take, record, post, share, publish, distribute, or threaten to distribute/public/share/send any:

[4] Any speech (being a communication in any form, whether in writing or otherwise) with the intention or likelihood of being threatening or abusive and likely to stir up hatred against any person or group of people because of their race, colour, nationality, religion, ethnic or national origin, membership of the Traveller Community, sexual orientation or gender.

- Image or content that could embarrass or humiliate or harass another person or group of people,
- Hate speech that could stir up hate against another person or group of people,
- explicit self-generated images[5] (including intimate images and/or nudes),
- sexually explicit images of yourself or of another person,
- child-abuse images,
- intimate images or revenge porn[6],
- grossly offensive, explicit, or sexually explicit image that could cause harm or distress or humiliation to another person.

Any such content (media, post, words, photos, videos, recordings etc) found or stored on the Device may result in the School commencing a Code of Behaviour process, and could include the matter being reported to An Garda Síochána and/or TUSLA (Child and Family Agency).

(a) Copyright/IP: Students are allowed to have music and music apps on their device (eg. Spotify) provided there is no abuse or misuse or violation of copyright and/or intellectual property rights. The items downloaded and synchronized to a Device must comply with all laws.

(b) Students shall not use their Device or IT to plagiarise other people's work, and shall not access any site or chatroom or app selling pre-written term papers, book reports, or other forms of student work and attempt to "pass them off" as their own work.

(c) Students shall not send mass emails, or unsolicited emails, or junk emails, or spam[7], or do any other act or thing that would breach the ePrivacy Regulation (S.336/2011). S.I. No. 336/2011 - European Communities (Electronic Communications Networks and

[5] Students and their parents/guardians/care-givers are advised to read the resource "Information and Resources for Schools Around the Sharing of Explicit Self-Generated Images" published by the Professional Development Service for Teachers (PDST) and available at www.pdst.ie/sites/default/files/Lockers%20Updated.pdf

[6] Harassment, Harmful Communications and Related Offences Act 2020

[7] Unsolicited (ie unrequested) messages, including those that are a nuisance to or unwanted by the recipient.

Services) (Privacy and Electronic Communications) Regulations 2011.

4.13 **I understand that my Device is subject to monitoring and inspection without notice, and I consent to same**

(a) Internet searches while using School IT are monitored using the SENSO monitoring software. See further Appendix 1 for more detailed information about SENSO monitoring (Fair Processing Notice). This means that website access and internet activity on the Device is monitored in real-time. This is for the School to ensure student safety, and detect unlawful or harmful activity.

(b) IT is a privilege for the purpose of educational use only. So any student who accidentally searches for a search term they did not intend to, or did not understand its meaning, or retrieves information, or otherwise clicks on a link they should not have, in a way that would breach the standards of this AUP should immediately contact a Teacher for support as that activity will be identified by the SENSO monitoring. The Student should immediately link-in with a Teacher for support and to resolve the issue.

(c) Students should not search for or access sites that are inappropriate, (eg. porn, extremist or hate-speech content, content that advocates for violence or discrimination towards certain groups, or promotes self-harm or eating disordered content etc).

(d) Devices shall be subject to Monitoring during school hours (8.45am to 3:15pm) in either manual monitoring form (ie student required to hand over Device) or in system monitoring format (SENSO software – see Appendix 1 Fair Processing Notice) to ensure each Student is on-task with their classwork.

(e) It shall be a breach of the AUP to fail to co-operate with monitoring, or to fail to co-operate with any School investigation regarding breach of the AUP.

(f) **SENSO Real-time classroom monitoring:** The SENSO software helps to limit distractions and assists Teachers in stepping in if Devices are not being used for classroom activities. The classroom management tools including giving the class teacher an overview of what students are working on with the Sensor "Live Thumbnail View feature" teachers have the ability to view the screens of multiple students within the class in real-time.

(g) **SENSO AI driven threat analysis**: The SENSO software highlights if a Student accesses or types any content which may be harmful or inappropriate. This provides parents/guardians reassurance that the Student is being kept safe and protected when using their Device in School.

(h) The School shall support students in understanding what sort of search terms or search phrases might be considered harmful or illegal. In particular, teachers/Year Heads shall provide illustrative examples of the sort of search terms would trigger the SENSO software and generate alerts. The School understands that Students are curious and inquisitive about the world around them, and that Secondary School is a time to learn including through making mistakes. SHS School provides support to assist students in understanding how to be responsible when they have the privilege of using the Devices and IT.

Very Important: if the SENSO monitoring detects that a student was searching for or accessing harmful, illegal, offensive, or otherwise worrying materials (eg. porn, child abuse images, terrorism, extremist or hate-speech content, content that advocates for violence or discrimination towards certain groups, or self-harm, eating disorder content etc) an alert will be sent by the SENSO software to SHS senior management for action to be taken.

The School has a duty of care to students, and shall intervene where necessary. The SENSO software will not catch everything, and parents/guardians should understand the limits of the monitoring capabilities. Certain matters may trigger mandatory reporting obligations to An Garda Síochána and/or TUSLA, and Students/parents/guardians must understand that the School will have no choice but to comply with mandatory reporting laws where the circumstances warrant.

5. Parent/Guardian Responsibilities:

Parents/Guardians and Schools work in partnership to deliver education to Students. Parents/Guardians shall support the School’s AUP in the following ways:

5.1. To support their child in understanding, observing, and following the Standards.

5.2. To encourage their child to articulate/voice any worry they are experiencing, and contact a teacher/Year Head if they have any concerns regarding their child’s health or mental welling concerning use of the Device.

5.3. Provide a protective case that has corner protectors to mitigate the risk of damage to the Device.

5.4. Parents should be aware of the limitations of the SENSO Software (both in terms of time and ability). SENSO will not be monitoring the Device out-of-school hours, on weekends, out-of-term, and/or during the summer holidays. The SENSO monitoring is only applied during school hours on school days. Furthermore, the SENSO monitoring is not comprehensive and will not catch/detect every search/online activity that might be harmful or upsetting to a student. Parents should monitor students’ use of the Device when not in school particularly during homework and study times. Parents should inspect the Device and IT and other installed apps on a regular basis to ensure that there is no inappropriate material/use.

5.5. It is the parent/guardian’s responsibility to ensure that their child has removed any unapproved Apps from the Device prior to return to school in September.

5.6. It is the responsibility of parents/guardians to ensure that appropriate insurance cover is in place to cover any damage to the Device (including accidental damage). Failure to do so could result in the student being without a device for essential schoolwork until it is repaired or replaced by parents/guardians. The school is not responsible for any loss or damage to students’ property.

5.7. Parents should inspect the device to ensure that it is in good working order. Any technical issues can be reported immediately to Year Head or Principal by email.

5.8. Parents should immediately report any damage, interference or any concerns regarding bullying relating to or concerning the Device. Further information can be found in the school's Anti-Bullying Policy, and/or by contacting the Year Head or Principal.

5.9. Parents agree and consent to the inspection of the Device where or when deemed necessary by the ICT team and/or a Teacher and/or SHS senior management team. As part of the Code of Behaviour, Parents accept that the AUP consequences of misuse or breach shall include restriction to or limitation of access to the Device or any IT.

6. Consequences

6.1. Students who breach this AUP (including by falling short of the expected Standards) will be subject to the School Code of Behaviour. The school applies a ladder of sanctions depending on the seriousness of the breach and the adverse effect the breach has had on other people. It is hoped that by setting out such clear Standards that Students will understand what is expected of them, and that positive strategies will obviate the need for sanction under the Code of Behaviour. However, in more serious cases, the School will have no choice but to invoke the Code of Behaviour which could lead to a student being suspended and/or expelled.

6.2. In addition to any processes and/or sanctions as may be applied under the Code of Behaviour, any breach of the AUP may result in any or all of the following (in whole or in part) being imposed, depending on the seriousness of the breach and/or the harm caused. The School shall have regard to all the circumstances in determining what is fair and appropriate:

(a) A student may be referred to the School Counsellor for support, and/or referred to TUSLA (Child and Family Agency) by way of child protection or child welfare referral pursuant to the Department of Education Child Protection Procedures and/or Children First Act 2015 and/or Children First National Guidance 2017.

(b) The Student's parent(s)/Guardian(s) may be notified in appropriate circumstances. The School has authority to contact the Student's parent(s) and/or guardian(s) in appropriate circumstances, and notify them of what has occurred.

(c) A student may be put on restricted use and/or limited access to or of the Device or IT, at the Principal's/Deputy Principal's discretion. Such restriction or limitation may be limited in time (eg. during the school day, for a number of school days) (this shall be called "Restrictions" for brevity).

(d) A student's device can be confiscated at the Principal's/Deputy Principal's discretion. Such confiscation may be limited in time (eg. during the school day, for a number of school days, or until a certain condition is satisfied).

(e) The school authorities have authority to delete inappropriate material from any Student's Device (if applicable) and/or to prevent/block the installation of certain apps and/or to otherwise restrict/limit the student's use of the Device and/or IT.

(f) A student may be subjected to conditions/limitations around use of Device and/or IT as the Principal/Deputy Principal determines in their discretion;

(g) A student may be required to do some action (eg. apologise) or refrain from doing something (eg. refrain from disrespectful online behaviour).

(h) As already stated in the AUP, certain matters may trigger mandatory reporting laws, and if that is the case the student's behaviour or activities shall be reported to An Garda Síochána and/or TUSLA (Child and Family Agency).

(i) If appropriate, the student's behaviour and/or conduct shall be dealt with under the School's Code of Behaviour. Sanctions under the Code of Behaviour include but are not limited to suspension and/or expulsion.

Please note that the School is not obliged to implement the above consequences in any sequence; nor does the School have to exhaust one set of consequences before imposing another. Rather the School shall impose any one (or any blend of one or more) of the above consequences where proportionate to the seriousness of the breach.

Ratified by the Board of Management on:

June 2023

Review Date: 9/2/2023

Parents' /Guardians' Agreement:

We have read and understood the AUP hereby agree to same. We grant to the School (and its staff) the right to inspect and monitor our child's Device and IT use, to monitor compliance with the AUP, and we Consent to the SENSO monitoring software. We agree to assist our child in understanding and observing the Standards. We understand the School will impose Consequences if there is any breach or non-observance of the Standards.

Name of Parent/Guardian: ________________________

Signature of Parent/Guardian: _____________________

Date: __________________________

Name of Student: _____________Class: Year:

Signature of Student: ____________________

Date: _____________________

Student Agreement

I will behave ethically and responsibly

I will never leave the Device unattended. I will know where my Device is at all times.

I will never lend my Device to someone else

I will respect that IT is a privilege for class use (and for SHS Students only)

I will take good care of my Device and be responsible for my use of my Device. I will charge my Device battery every night.

I will not disassemble any part of my Device, personally attempt any IT repairs, or attempt to undermine SHS IT security

I will be responsible for my health and mental wellbeing while using my Device

I will only photograph people with their permission. I will only use the camera or the microphone when my teacher tells me to.

I will not use my device in toilets or dressing rooms, and I will respect other people's privacy

I will not use my Device or School IT for financial or commercial gain.

I will not use my Device to bully, intimidate, harass, humiliate, hurt, defame or abuse others

I will not use School IT to access or search for illegal or harmful content, or to conduct any illegal activity, or otherwise break the law

I understand that my Device is subject to monitoring and inspection without notice, and I consent to same

Student Name: _____________________Class: Year:

Signature: _____________________________

Date: ____________________

Appendix 1

SENSO fair processing notice