Ursuline High School
Personally Owned Device Policy

As stated in the Student Technology and Internet Acceptable Use Policy (STIAUP), the schools in the Diocese of Youngstown maintain computer systems and networks (information and communication resources) as a part of its mission to promote excellence in education and to enhance students' productivity, efficiency and effectiveness with communication and resource sharing.

Ursuline High School will permit students to bring a Personally Owned Device (POD) to use during the school day for educational purposes. Students must be committed to digital citizenship and use technology resources in ways that promote an educational environment that follows the philosophy, principles and teachings of Ursuline High School. All users are subject to legal requirements as well. **Students and parents or guardians must sign the Personally Owned Device Policy Agreement to be permitted to use such devices in school.**

Students and parents or guardians accept full responsibility for the security, maintenance, and repair of their own POD. Personally Owned Devices *may* include but are not limited to:

- computers – laptops, iPads, netbooks, notebooks or tablets
- peripheral equipment – disk drives, ear buds, mice, etc.
- other electronic equipment – MP3 players, iPods, video/audio equipment, cameras, etc.
- cell phones
- e-readers
- translators
- information storage devices such as USB devices, CDs, etc.

Systems and resources also considered in this policy are

- The school network including local area networks, wireless networks, network connections to remote sites, etc.
- All software or programs administered by the school or running on school resources, such as email, web browsers, file exchange software, databases, web programs, etc.

Responsibility, Safety and Security

Students who bring a POD to school or on school property are responsible for securing them at all times. If a POD appears to have been stolen, the student should immediately report the incident to the assistant principal, but the school does not accept responsibility for a student's POD.

The safety and security of the students and the network are our primary concern, and students are required to work with the teaching staff and administrators to protect fellow students, electronic devices and systems. Security on any computer system is a high priority, especially when the system involves many users. If a student identifies a security problem involving him/herself or another student, they are to report it to the assistant principal.

Security measures, such as filters and virus protection software, are not to be bypassed by using personal data plans. Compliance to the *Child Internet Protection Act* as referred to in the

Student Technology and Internet Acceptable Use Policy is a must (see link to ORC § 3314.21). The school may take disciplinary action against students found violating this policy.

Privileges

The use of school Internet accounts and equipment is a privilege and may be revoked for misuse or violation of policies by the administration, teachers, or another designated school official.

Privacy

There is **no** expectation of privacy with the use of personal devices that access the school network or used in school. All Information Technology (IT) systems and networks and all messages or documents composed, sent or received on these systems are and remain the property of the school.

Expectations

As a student of the Diocese of Youngstown and Ursuline High School I agree to:

- use the school wireless network at all times. Students ***may not use personal data plans*** (2g, 3g or faster) due to safety and security reasons (see link to ORC § 3314.21).
- keep my PODs with me or locked in my locker.
- keep PODs in protective cases at all times while on school property.
- back-up all work on a daily basis to cloud storage, personal flash drive, home computer or storage device. Information is not to be stored on school systems.
- use a POD in a classroom only with explicit teacher approval and supervision.
- follow all rules in the Student Technology and Internet Acceptable Use Policy (STIAUP).
- adhere to any additional guidelines that the classroom teaching staff or other school personnel may require including connection to the Internet or using Apps, games, etc.
- in no way use a POD to disrupt or distract from the learning environment.
- in no way use a POD to interfere with the academic performance of myself or another student.
- not use resource intensive applications, programs, etc. that take up an unusual amount of bandwidth (music and video sharing programs like You Tube and Pandora).
- come to school with a fully charged device and not rely on school outlets.
- not take or transmit pictures or video on any camera or video enabled device without express consent of a school official.
- not take or transmit pictures or video on any camera or video enabled device that violates the philosophy, principles and/or teachings of the Diocese of Youngstown or the Roman Catholic Church.
- not take or transmit pictures or video on any camera or video enabled device that violates diocesan and school policy, the Student Code of Conduct, or civil law.
- respect and guard the privacy of myself and others by not posting last names on the Internet through email or any social networking system or group and then, only when, permission is explicitly given by school officials, students, parents or guardians.
- adhere to copyright laws (not duplicating text, licensed software or related documents as stated in the STIAUP).
- refrain from making **personal contact** during class time that is **unrelated to school business** with any type of device or means (through text, email, Skype or similar, etc.). The exception would be to contact a relative or responsible party to pass on crucial

information. This is done strictly with permission given by a school official. Voice conversations are always prohibited during school hours.
- refrain from sending any message by any means (text, email, etc.) that you would not want read by a third party (student or adult).
- keep my device muted or in a silent mode

The school reserves the right to audit and monitor usage of these resources and to access, view and disclose their contents, with or without notice or the consent of the user and with or without cause.

Students must surrender their PODs to any authorized personnel upon request and must allow these authorized personnel to examine the POD to determine whether established policies have been violated.

Liability

Parents are encouraged to add personally owned devices to their homeowner's or renter's insurance. The Diocese of Youngstown and Ursuline High School assume no responsibility or financial liability for any damage or loss the student or parent suffers, including but not limited to theft, physical damage or lost POD's, software malfunction or loss of data on the POD. Again, students who bring a POD on campus are responsible for securing them at all times and take full responsibility for their protection.

- Ursuline High School assumes no responsibility for lost or corrupted work due to failure to back-up or due to non-operation of a POD.
- Classroom teachers set policy for any work that is incomplete due to POD failure or work that is lost by any means.
- Repair, upgrades and maintenance are the responsibility of the owner of the device.
- Students and parents or guardians are responsible for maintaining their virus protection and setting the POD to automatic update and scanning. The Department of Educational Technology maintains a page listing free and open source **Anti-Virus and Firewalls** software at the following link: http://goo.gl/6xqJs. This page includes freely available computer anti-virus programs.
- Ursuline High School will not support hardware or software issues with non-school purchased personal computers, printers, or peripherals at school.
- The Diocese of Youngstown and Ursuline High School will not be responsible, financially or otherwise, for unauthorized transactions conducted at school and over the school network.

The Diocese of Youngstown and Ursuline High School take available precautions and use firewalls and filters to restrict/limit access to controversial materials and also have alerted students to the risks of the Internet and the use of computer/telecommunications devices; however, on a global network it is impossible to control all communication and materials.

Regulations and Guidelines

Security, Safety and Privacy Violations, both Policy and Legal, when Using a POD at School

As a student of the Diocese of Youngstown and Ursuline High School I agree to not:

- take pictures, videos, or recordings of students, faculty, teaching staff or administrators with a POD without their knowledge and permission;
- bypass the school filtered network to access the internet;
- destroy, intrude upon or harm the network monitoring software or applications;

- violate copyright laws or plagiarize;
- use a device for any type of cheating as referred to in the STIAUP; and
- use a device for personal purchases of any kind while on school premises.

Violations of the above guidelines will be considered a **serious violation** of the school's POD Policy.

As a student of the Diocese of Youngstown and Ursuline High School I understand:

- PODs may be used in classrooms as directed by teachers with the primary usage always relating to instruction.
- PODs may be used in studyhall, the library/learning center or cafeteria. Earbuds are required for MP3 Players and must be at a volume that does not disrupt others.
- Voice communication on a cell phone is **never** permitted during the school day.
- PODs may NOT be used during liturgies, prayer services, or assemblies.

Using a POD that violates the above conditions will be considered a **minor violation** of the school's POD Policy

Any violation of security, safety and privacy regulations and rules of Ursuline High School and/or Diocese or civil law, when using a POD at school, may also *subject a student to disciplinary and legal action as listed in the Student Technology and Internet Acceptable Use Policy (STIAUP).*

Network access and PODs is a privilege that may be revoked for any reason at the discretion of the administration.

Security, Safety and Privacy Violations Regarding Blogging, Wikis and Using Social Networking

*Students should be creative, thoughtful, and proactive in building **digital footprints** that contribute to their personal growth. Students should act in a way that makes their parents, the Diocese of Youngstown and Ursuline High School proud. Students should be aware that colleges and universities, scholarship committees, potential employers, and internship supervisors may monitor these sites as a way of assessing and selecting applicants.*

As with any electronic communication, blogging, wikis and social networking paths have value in a school environment when used for collaboration and communication between students about educational materials. When using these internet resources, students must be committed to digital citizenship and use technology resources in ways that promote an educational environment that follows the philosophy, principles and teachings of Ursuline High School, the Diocese of Youngstown and the Roman Catholic Church.

Rules and regulations for participating in social networking are for activity done both in and out of school when such: a.) creates a hostile environment; b.) infringes on the rights of staff or student(s) at the school; and c.) disrupts the educational process or the orderly operation of a school. Text or photos placed online should be considered by the user as a public document or image. The school Student Code of Conduct and all technology related policies apply. All users are subject to civil laws as well. Students are to report any misuse of the network to a teacher or administrator.

As a student of the Diocese of Youngstown and Ursuline High School I agree to not:

- transmit hurtful or damaging information or comments as outlined in the STIAUP to mistreat, embarrass or disrespect any member of the school community;
- transmit and display/share personal information, inappropriate images or content using a POD of students, faculty, teaching staff or administrative staff;
- post or share falsified information using a POD regarding students, faculty, teaching staff or administrative staff;
- use names, initials, logos, pictures, or representations of the students, faculty, administration or other individuals that, in the determination of the school administration, are degrading, lewd, threatening or inappropriate including but not limited to comments, cartoons, jokes, unwelcome propositions or love letters;
- access any Internet site deemed inappropriate by the administration;
- engage in conduct that violates safety, security and privacy regulations and guidelines in this policy and the STIAUP (e.g., any forum to intentionally mistreat, embarrass or disrespect other students, families, alumni, faculty, administration or other members of the school community); or
- electronically transmit any material in violation of school policy or any federal or state laws or regulation.

Violations of the above guidelines will be considered a **serious violation** of the school's POD Policy.

Teaching staff and administrators have the right to deny student's access to blogs, wikis and social networks at school if inappropriate behavior is evidenced including poor network etiquette.

Accepted Rules of Network Etiquette

Students must be committed to using digital citizenship when using technology resources by applying **network etiquette whether personally owned or school owned**. Network etiquette is another practice that ensures an educational environment that follows the philosophy, principles and teachings of the Roman Catholic Church. Network etiquette includes

- ***Being Polite*:** Remember, what is written or posted can be viewed globally;
- Using ***appropriate language*** *and* ***refraining from making offensive remarks*** *and* ***sharing offensive material***;
- ***Respecting Privacy*:** Remember, email and other postings on the Internet are not guaranteed to be private. You and others are put at risk when personal information is shared on the Internet.
- **Connecting fairly**: Avoid slowing the network.

Definitions:

- **Blogging** is written postings or other content on a publicly available Internet site by an individual and includes photographs, drawings, videos, or any other graphic or audio information. "Video-blogging" (live and/or taped video content) broadcast on the Internet.
- **Social Networking** is texting, instant messaging, Facebook, Twitter, MySpace, LinkedIn, Instagram, Vine, Snapchat, or similar used for communicating with other individuals.

Consequences

Minor violations of the POD Policy will result in the following penalties from the classroom teacher, administrator, or supervisor of the study hall, cafeteria, or library/learning center.

1. The student's POD will be confiscated until the end of the period.
2. The student will sign a conduct card for violation of POD Policy with a penalty of 5 conduct points and 1 detention.

Serious violations of the POD Policy will result in one or more of the following penalties and will be assessed at the discretion of the school administration:
1. The student's POD will be confiscated.
2. Students will face suspension or revocation of computing and other technological privileges.
2. Students will face disciplinary action assigned by the Assistant Principal, including a conference with the student's parents.
3. Students will face other legal action including action to recover damages.
4. Students will face referral to law enforcement agencies.

In addition:

- Deliberate or careless transmission, publication or postings of person's private information, falsifying information and posting inappropriate or harmful material as outlined in the STIAUP will result in disciplinary action up to and including expulsion.
- Bypassing the network monitoring software or applications considered intrusive by the school is a serious offense, and will result in disciplinary action, up to and including expulsion.

In some circumstances parents can be held responsible for student's acts according to Ohio law. Students and parents or guardians must sign the Personally Owned Device Policy Agreement before a student will be permitted to use such devices and the Internet at school. In granting this permission, parents/guardians and students release any and all claims against the Diocese and school for damages, theft or loss of Personally Owned Devices and their peripheral components.

If as a parent or guardian you do not consent to having your student use a personally owned device in school, you may verify that information by sending a written letter stating such.

Links

http://transition.fcc.gov/cgb/consumerfacts/cipa.pdf *Children's Internet and Protection Act* and Protecting Children in the 21st Century Act

Ohio Revised Code §§ *3314.21* on web content filtering

Ohio Revised Code §§ 2917.21(A), 2913.01(Y) on cyber-bullying

https://www.ohiobar.org/ForPublic/Resources/LawFactsPamphlets/Pages/LawFactsPamphlet-23.aspx See "**What should I know about my children's Internet use?"**

http://www.coppa.org/coppa.htm See part (4) (A) and (B) Children's Online Privacy Protection Act (COPPA)

www.copyright.gov/fls/fl102.html Copyright Law and United States Fair Use

Ursuline High School

Student Personally Owned Device Policy Agreement

I understand and agree to abide by the terms of the Ursuline High School Student Personally Owned Device Policy. I understand that when I am using Personally Owned Devices at school and accessing the Internet, I am responsible for safeguarding and maintaining my own device. I must respect myself, others and the property of the school or others; adhere to all rules of courtesy and etiquette laws as prescribed by federal, state, or local governments, and all Diocese of Youngstown and Ursuline High School rules and policies.

I understand that Internet access or school network access, whether in school or through remote connections, is to be used for educational purposes only.

_____ Date _____/_____/_____

(To be signed by student)

Grade _____

Parent and Guardian
Student Personally Owned Device Policy Agreement

As the parent or guardian of this student, I have read the Ursuline High School Personally Owned Device Policy and agree to its terms. I will instruct my child regarding any risks, responsibilities and regulations and the importance of following rules for personal safety and security and the safety and security of others.

I hereby give my permission for _____ to

(student's name)

use a personally owned device in school and access the school's Internet network. I understand that my child has agreed not to access inappropriate material on the Internet, damage property or cause harm to others. I understand that Ursuline High School or Diocese of Youngstown is not held liable for theft, loss or damage of personally owned devices and their peripheral components that are located on school property. I will emphasize to my child that he or she is responsible for safeguarding and maintaining his or her own device.

Parent/Guardian Printed Name: _____

Parent/Guardian Signature: _____

Return to your homeroom teacher by Friday, August 25.