Appendix C
Cyber-Bullying Policy for
Catholic Schools and Academies of the Diocese of Brooklyn
February 2019

1. Purpose:

One of the main duties of the schools and academies within the Diocese of Brooklyn is to provide a safe environment for our students. With the current state of technology, internet use and digital communications, this extends beyond the bounds of the physical building. Students now have 24x7 access to each other through computers, smart phones and tablet devices which can provide both an enriching experience for learning and an unfortunate opportunity for mischief. The Diocese of Brooklyn, in an attempt to harness the good and discourage and protect from the bad, has developed the following policy and guidelines to govern cyber-bullying.

2. Scope of Use:

This policy applies to the use of technology both inside and outside of the school/academy. When personal outside use of a technology violates this policy in whole or in part, these actions may be subject to disciplinary measures found within.

3. Definitions of Cyber-Bullying:

The following are types of cyber-bullying that can occur. This is not a comprehensive list of every action that can be deemed cyber-bullying, and items may be removed or added without prior notice. This listing is adapted from the New York State Department of Justice Definition of Cyber-Bullying.

1. **Flaming –** The act of posting electronic messages that are deliberately hostile, insulting, mean, angry or vulgar to one or more persons either privately or publicly to an online group
2. **Denigration –** Occurs when a person sends or publishes cruel rumors, gossip or untrue statements about a person to intentionally damage the victims reputation or friendships.
3. **Bash Boards –** Online bulletin boards or forums where people post anything they choose. Generally, postings are mean, hateful and malicious.
4. **Impersonation –** The act of posing as or pretending to be another person. This can either be through a malicious attack resulting in the takeover of an existing account (hacked/stolen credentials) or through the creation of a fake account in someone else's name. Considerable damage can be done through this time of attack to the victim's reputation and relationships.
5. **Outing –** Occurs when confidential, private or embarrassing information is posted or shared publicly. Can include the forwarding of email messages, text messages or photos meant to be private to an unintended third party recipient(s).
6. **Trickery –** The act of tricking someone into divulging personal, embarrassing or private information either publicly or to a person who then uses that information for malicious intents. Information gained can be used to blackmail, post publicly online or for person gains depending upon the information.

7. **Exclusion –** An indirect method of cyber-bullying in which someone is intentionally excluded from and online group, community or activity.
8. **Harassment –** The act of sending repeated insulting, hurtful, rude or vulgar message
9. **Happy Slapping –** a real world attack which is recorded and then posted online. Often referred to as a practical joke by the attackers, hence the term "happy slapping"
10. **Text Wars or Attacks –** When several people gang up on a victim sending the target repeated emails and text messages resulting in emotional and possibly financial damage for data and messaging costs
11. **Online Polls –** potentially harmful or demeaning, they can contain malicious questions such as "Who is the ugliest person in 8th grade?" or "Who do you love to hate?"
12. **Sending Malicious Code –** When intentionally perpetrated with malicious intent, can be used for spying, tracking, stalking, or to harm devices or the victim themselves
13. **Images and Videos -** Due to the prevalence and accessibility of camera cell phones, photographs and videos of unsuspecting victims, taken in bathrooms, locker rooms or other compromising situations, are being distributed electronically. Some images are emailed to other people, while others are published on video sites such as *YouTube*.
14. **Griefing –** Chronically causing grief to other members of an online community or intentionally disrupting the immersion of another in their game play
15. **Trolling –** Lurking or "trolling" message boards and forums for the purpose of defaming, "flaming", annoying, embarrassing or otherwise being hostile to users through public posts. The victim may or may not be known to the "troll" and "trolls" are often able to act anonymously.

4. <u>Responsibilities of the School/Academy</u>:

In accordance with New York State Law on Cyber-Bullying, inappropriate, defamatory, or content found to be injurious to a school/academy community member may result in disciplinary action, even if done outside of school/academy premises or using devices not owned or controlled by the school/academy. All instances of such behavior must be reported immediately to the administration, who will investigate the matter and enforce the consequences deemed appropriate.

- Monitoring of communications of minors when using electronic mail, chat rooms and other forms of direct electronic communication
- Unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- Measures restricting minors' access to materials harmful to them
- Educate students on cyber-bullying to encourage them to identify bullying behavior, avoid exhibiting the behavior and keep themselves from being the victim of bullying behavior.
- Provide guidance and counsel students on both sides of the conflict.

School/Academy administrators, faculty and staff are responsible to ensure activities involving students do not harbor or promote cyber-bullying in any way. Inadvertent exclusion or inappropriate comments that go unseen can quickly become a serious situation. What may seem like a harmless joke in class or online could begin a cycle of bullying, or be a sign of something much larger that has been going on.

5. **Responsibility of Students:**

As a member of the Diocese of Brooklyn community, students are expected to act in accordance with the tenants of the Catholic Church. This includes conducting yourself in an appropriate manner in the digital realm and treating others and yourself with respect, kindness and understanding. It is imperative for each student to ensure that this is protected for both themselves and other members of their school/academy community. The following are guidelines to help students protect themselves and others and recognize situations and how to handle them.

Protecting Yourself from Cyber-Bullying and Cyber-Attacks

- Do not share personal information over the internet that could be used to facilitate an attack
- Never share account credentials with anyone other than your parents or guardians
- If you are being harassed by someone, report the user to the appropriate administrator (such as Facebook or Twitter), tell your parent/guardian immediately and do your best to take screenshots or print the offensive material to document the incident
- If the person is a member of your school/academy community, also inform the school of the incident providing any documentation that you can
- Block users who engage in bullying behavior from contacting you
- Set social media accounts such that posts need approval before they can be seen publicly on your page (Facebook, Twitter, Instagram, etc.)
- Do not engage others who are looking to "bait" you into an altercation. This is often a tactic to lure victims into revealing information that is then used for the attack
- Avoid aggressive behavior that could provoke others to retaliate

Protecting Others from Cyber-Bullying

- Do not participate in any of the behaviors outlined in the definition above
- When communicating digitally, be mindful to show respect and understanding
- Refrain from using derogatory, defaming, embarrassing or vulgar language when communicating
- Report any aggressive behavior observed to the appropriate administrator, and your parent or guardian
- If it involves members of the school/academy community, inform the school as well with any documentation you can provide
- Discourage others who may be thinking, planning or talking after the fact about cyber-bullying or attacks they have/will engage(d) in

Identifying Cyber-Bullying

It is important to understand that not all undesirable interactions on the internet are cyber-bullying. By definition, bullying is a recurring behavior. Repeated attacks through email, forum posts, instant or text messages or the like constitute cyber-bullying. A single incident, while not condoned or accepted, is not cyber-bullying; unless it is ultimately deemed to be the first in a string of attacks. The instant transfer and duplicative nature of digital mediums expands the threat of cyber-bullying and must be considered in its identification. If an act deemed to be inappropriate is conducted even once, but is that shared and transmitted repeatedly over a

digital medium, that act crosses into a case of cyber-bullying even if it was the first/only occurrence and must be handled as such.

7. Policy Violations:

Violation of this policy in whole or in part may result in any or all of the following and will be issued at the discretion of the school/academy principal:

- Loss of use/privileges of school/academy technology.
- Disciplinary action including, but not limited to, detention, suspension, expulsion, and /or legal action by the school/academy, civil authorities, and/or other involved parties.
- Compensation for damages, both physical and punitive, incurred due to actions in violation of this AUP