Diocese of Dallas
Internet School Safety Policy

A guide for students, staff, parents, and visitors to use the internet safely and responsibly

Introduction

The internet is a powerful tool for learning, communication, and collaboration. It also poses some risks and challenges for the safety, privacy, and well-being of students, staff, and parents. This document outlines the Internet Safety Policy of our school, which aims to meet the regulatory requirements of the Children's Internet Protection Act (CIPA) and the Children's Online Privacy Protection Act (COPPA).

The Internet Safety Policy applies to all users of the school's network, devices, and online resources, whether on or off campus. The policy covers the following topics:

- Acceptable and responsible use of the internet
- Filtering and monitoring of online content
- Protection of personal information and data
- Educating and empowering students to be safe and responsible digital citizens
- Reporting and responding to cyberbullying, harassment, and inappropriate online behavior
- Enforcement and consequences of violating the policy

Acceptable and Responsible Use of the Internet

The school provides access to the internet for educational purposes only. Users are expected to use the internet in a manner that is consistent with the school's mission, values, and policies. Users are also expected to respect the rights and property of others, and to follow the laws and regulations that govern the use of the internet.

Some examples of acceptable and responsible use of the internet are:

- Using the internet to access, create, and share educational content and resources
- Using the internet to communicate and collaborate with teachers, classmates, and other learners
- Using the internet to research and explore topics related to the curriculum and personal interests

- Using the internet to develop and practice digital skills and literacy
- Using the internet to access and participate in online learning platforms and programs approved by the school

Some examples of unacceptable and irresponsible use of the internet are:

- Using the internet to access, create, or share content that is illegal, harmful, offensive, or inappropriate
- Using the internet to engage in cyberbullying, harassment, or discrimination
- Using the internet to cheat, plagiarize, or violate academic integrity
- Using the internet to disrupt, interfere, or damage the school's network, devices, or online resources
- Using the internet to download, install, or run unauthorized software, programs, or files
- Using the internet to access or participate in online platforms, programs, or activities that are not approved by the school
- Using the internet to access others' accounts

Filtering and Monitoring of Online Content

The school uses filtering and monitoring software to block or restrict access to online content that is deemed inappropriate, harmful, or illegal for students. The filtering and monitoring software is designed to comply with the requirements of CIPA, which mandates that schools prevent access to visual depictions of obscenity, child pornography, or material that is harmful to minors.

The filtering and monitoring software is not infallible and may not block all inappropriate or harmful content. Users are responsible for their own online behavior and choices, and should report any content that is inappropriate, harmful, or illegal to a teacher or administrator. Users should also avoid accessing or sharing any content that violates the Acceptable and Responsible Use of the Internet section of this policy.

The school reserves the right to monitor and review any online activity or content that is accessed, created, or shared by users on the school's network, devices, or online resources. The school may also monitor and review any online activity or content that is accessed, created, or shared by users on their own devices, if they are connected to the school's network or using the school's online resources. The school may use the monitoring and review data to ensure compliance with this policy, to investigate potential violations or incidents, or to provide feedback and guidance to users.

Protection of Personal Information and Data

The school is committed to protecting the personal information and data of users and complying with the requirements of COPPA. It protects the privacy of children under 13 years of age online.

The school collects, stores, and uses personal information and data of users for educational purposes only. The school does not disclose or share personal information and data of users with third parties, unless required by law or authorized by the user or their parent or guardian. The school also does not sell or rent personal information and data of users to third parties for any reason.

The school uses encryption, passwords, and other security measures to safeguard the personal information and data of users from unauthorized access, use, or disclosure. However, the school cannot guarantee the absolute security of personal information and data of users, and users are responsible for protecting their own personal information and data online.

Some examples of personal information and data that users should protect online are:

- Name, address, phone number, email address, or other contact information
- Birth date, age, gender, or other demographic information
- Social security number, student ID number, or other identification information
- Grades, test scores, transcripts, or other academic information
- Medical records, health conditions, or other health information
- Photos, videos, or other media that can identify the user or others
- Passwords, usernames, or other login information

Some examples of how users can protect their personal information and data online are:

- Using strong and unique passwords, and changing them regularly
- Not sharing passwords, usernames, or other login information with anyone
- Not using the same password, username, or other login information for multiple accounts or platforms
- Logging out of accounts or platforms when not in use
- Not clicking on links or opening attachments from unknown or suspicious sources
- Not responding to requests for personal information or data from unknown or suspicious sources and reporting to an adult when such request is made.
- Not posting or sharing personal information or data on public or unsecured platforms or networks
- Checking the privacy settings and policies of platforms or networks before using or joining them

- Asking for permission from parents, guardians, teachers, or administrators before providing or sharing personal information or data online

Educating and Empowering Students to be Safe and Responsible Digital Citizens

The school recognizes that educating and empowering students to be safe and responsible digital citizens is essential for their success and well-being in the digital age. The school provides opportunities for students to learn and practice digital skills and literacy, such as:

- Searching, evaluating, and using online information effectively and ethically
- Creating, publishing, and sharing online content respectfully and responsibly
- Communicating and collaborating online appropriately and productively
- Managing and balancing online time and activities healthily and wisely
- Protecting and respecting online privacy and security
- Understanding and following online rules and norms
- Recognizing and reporting online risks and threats
- Resolving and preventing online conflicts and issues
- Cyberbullying awareness

The school also encourages parents and guardians to be involved and supportive of their children's online learning and activities. The school provides resources and guidance for parents and guardians to help them:

- Monitor and supervise their children's online access and use
- Discuss and establish rules and expectations for their children's online behavior and choices
- Teach and model safe and responsible online habits and practices
- Support and assist their children with online learning and challenges
- Communicate and collaborate with the school on online safety and education issues

Reporting and Responding to Cyberbullying, Harassment, and Inappropriate Online Behavior

The school does not tolerate any form of cyberbullying, harassment, or inappropriate online behavior on or off campus. Cyberbullying, harassment, and inappropriate online behavior are defined as any online actions or communications that are intended to harm, threaten, intimidate, humiliate, or harass another person or group, or that create a hostile or offensive online environment.

Some examples of cyberbullying, harassment, and inappropriate online behavior are:

- Sending or posting mean, rude, or hateful messages or comments
- Spreading rumors, lies, or gossip online
- Sharing or posting embarrassing, private, or false information or images of another person or group
- Excluding, isolating, or discriminating against another person or group online
- Impersonating, hacking, or stealing another person's online identity or account
- Stalking, threatening, or blackmailing another person or group online
- Encouraging or inciting violence, self-harm, or illegal activities online

The school expects all users to report any cyberbullying, harassment, or inappropriate online behavior that they witness or experience to a teacher or administrator as soon as possible. The school also expects all users to cooperate and assist with any investigation or intervention of cyberbullying, harassment, or inappropriate online behavior.

The school will respond to any reports of cyberbullying, harassment, or inappropriate online behavior promptly and appropriately, in accordance with the school's policies and procedures. The school will take appropriate actions to stop, prevent, and address any cyberbullying, harassment, or inappropriate online behavior, such as:

- Removing or blocking access to the online content or platform involved
- Contacting and notifying the parents or guardians of the users involved
- Providing support and counseling to the users involved
- Applying disciplinary or legal consequences to the users involved
- Referring and/or reporting on the users involved to external agencies or authorities, especially as required by law.

Enforcement and Consequences of Violating the Policy

The school will enforce this policy and monitor compliance with this policy regularly and consistently. The school will use various methods and tools to enforce and monitor compliance with this policy, such as:

- Requiring acknowledgement and acceptance of this policy annually or as needed
- Providing training and education on this policy and its expectations to users
- Reviewing and updating this policy and its expectations periodically or as needed
- Using filtering and monitoring software to block or restrict access to inappropriate or harmful online content
- Using filtering and monitoring software to monitor and review online activity and content of users

- Conducting audits and inspections of the school's network, devices, and online resources
- Investigating and responding to any reports or incidents of policy violations

The school will apply appropriate consequences to any user who violates this policy, in accordance with the school's policies and procedures. The consequences will depend on the nature, severity, and frequency of the violation, and may include:

- Warning or reprimand
- Loss or restriction of online access or privileges
- Confiscation or suspension of device or account
- Restitution or compensation for damages or losses
- Detention or suspension
- Expulsion or dismissal
- Legal action or prosecution