With the use of technology, including the Internet, Intranet, hardware and software, [St. Mary's Charter School ("School") is expanding learning access for students, staff, and parents. With this opportunity comes the responsibility for appropriate use. The School's Acceptable Use Policy explains and defines responsible and ethical use of educational and administrative technology for all employees. All rules embodied herein are designed to guide employees in appropriate and acceptable use of School technology, and are designed to protect both the employee and the School. This policy also governs the use of the School's electronic mail accounts and employee-owned personal electronic devices, including laptops, portable and handheld computing devices, and cellular telephones.

Computers

The School's electronic communications systems, including its network and access to the Internet, are primarily for administrative and instructional purposes. Limited personal use of the system is permitted if the use:

1) Does not result in any direct cost paid with State funds, or if the School's charter holder is reimbursed for any direct costs involved;

2) Does not relate to private commercial purposes; and

3) Involves only incidental amounts of employee time, comparable to reasonable coffee breaks during the day.

Electronic Network Use Guidelines and Safety Policy

The operation of technology in the School system relies heavily on the proper conduct of users. Every School user has the responsibility to respect and protect the rights of every other user. School users are expected to act in a responsible, ethical and legal manner, in accordance with the missions and purposes of the school.

The School's computer systems are for use by authorized individuals only. Any unauthorized access to these systems is prohibited and is subject to criminal and civil penalties. Use of any network or computing resources must be consistent with the rules appropriate to that network.

All network users are expected to use moral and ethical guidelines in making appropriate decisions regarding network use. Use of the School network is a privilege, not a right, and inappropriate use will result in cancellation of that privilege, disciplinary action, and/or prosecution. Prior to participation, a potential network user will receive information pertaining to the proper use of the network and sign a user agreement. School administrators will decide what constitutes inappropriate use of the network;

their decision is final. Violations will be dealt with in accordance with the School's Student Code of Conduct or Employee Handbook, or local, state, or federal law.

Unacceptable conduct on the School network includes, but is not limited to:

- Using the network for any illegal activity including, but not limited to, "hacking," copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering.
- Transmitting material in violation of any federal, state, or local law or School policy.
- Using School technology for financial or commercial or personal gain.
- Degrading or disrupting equipment or system performance.
- Vandalizing hardware.
- Viewing, copying, altering, or destroying data, software, documentation, or data communications belonging to the School or another individual without authorized permission.
- Unauthorized use of School resources, including hardware (*i.e.*, digital camera, projector, etc.) and printers for reasons other than job-related duties or School business.
- Adding unauthorized personal computers, printers, and/or software to the School network.
- Gaining unauthorized access to resources or entities.
- Invading the privacy of individuals.
- Using another individual's user-name and password.
- Disclosing a system password to another employee or student, or attempting to disclose another employee's or student's password.
- Placing of unlawful information on a system.
- Using the School network for political lobbying.
- Intentionally accessing pornographic, inappropriate, or unauthorized material either directly or in proxy.
- Intentionally bypassing the School's network systems and/or policies.
- Intentionally transmitting viruses or making changes that may result in the loss of an individual's work or access to the School network.
- Chain letters of any type that would cause congestion of the School network or otherwise interfere with the work of others.
- Installing software onto computers without appropriate approval.
- Paying access fees or committing School financial resources without formal authorization.

Security – Security is a high priority due to the number of users. Computer security cannot be made perfect, and it is likely that a determined user could access computer resources for inappropriate purposes or that an inquisitive user could encounter unacceptable material. Identified security problems should be reported to a system administrator or appropriate supervisor immediately and not shared with other users. Attempts to log on as another user may result in cancellation of user privileges. Any user identified as a security risk will be denied access to the system.

Vandalism – Vandalism is defined as any deliberate attempt to harm or destroy data or property of the School or another network user, the Internet/Intranet, or other networks. This includes the creation of or uploading of computer viruses to the Internet/Intranet or host site and destruction of hardware. Vandalism will result in cancellation of user privileges.

Online Harassment – Online harassment is defined as using the name or persona of another individual to create a web page on or to post one or more messages on a commercial networking site without obtaining the other individual's consent with the intent to harm, defraud, intimidate, or threaten any person. Online harassment also includes sending an electronic mail, instant message, text message, or similar communication that references a name, domain address, phone number, or other item of identifying information belonging to any individual without obtaining the individual's consent with the intent to harm or defraud any person and to cause the recipient of the communication to reasonably believe that the other individual authorized or transmitted the intention.

Cyber-Bullying – Cyber-bullying is defined as a situation where a child, preteen, or teen is tormented, threatened, harassed, humiliated, embarrassed, or otherwise targeted by another individual using the Internet, interactive and digital technologies, or mobile phones. Users of the School network are expected to refrain from such conduct.

Installing Software – Use of computer software is governed by copyright laws and network configurations. Care must be taken to avoid copyright violations and disruptions of the network related to incompatible or corrupted software; therefore, installation of any program or application onto any computer with access to the School's electronic network must be approved by the Campus Principal or designee.

Monitoring – All computers are the property of the School and are subject to searches or removal at any time. There is no privacy on the School network. The School will monitor any e-mail, network, and Internet activity occurring on School equipment or accounts. Anyone using the School network expressly consents to such monitoring. The School currently employs filtering software to limit access to sites on the Internet. If

the School discovers activities that do not comply with applicable law or school policy, prosecution and/or termination of user privileges will occur without warning.

E-mail Retention – Employees are required by law to retain certain e-mails, including communications referring to students made to parents, administrators, or law enforcement officials. Employees are responsible for archiving such communications.

Internet Safety – It shall be the responsibility of all School staff to educate, supervise, and monitor appropriate usage of the School network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Use of the Internet and other telecommunication activities must be in support of education and research that is consistent with the educational goals, objectives, and policies of the School.

In the classroom, student access to and use of the Internet will be under teacher direction and will be monitored as any other classroom activity. However, it is impossible to control all materials on a global network and users may encounter inappropriate or objectionable information. Even with filtering, the School cannot prevent the possibility that some users may access material that is not consistent with the educational mission, goals, and policies of the school.

Each School computer with Internet access shall have a filtering device or software that blocks access to visual depictions that are obscene, child pornography, inappropriate for students, or to any material deemed harmful to minors as defined by the Children's Internet Protection Act and as determined by the Campus Principal or designee.

The School Electronic Mail System

Electronic mail is a critical mechanism for communications at the School. However, use of the School's network, Internet, and electronic mails systems and services are a privilege, not a right, and therefore must be used with respect and in accordance with the goals of the School.

The objectives of this policy are to outline appropriate and inappropriate use of the School's electronic mail systems and services in order to minimize disruptions to services and activities, as well as to comply with applicable policies and laws.

Electronic mail access at the School is controlled through individual accounts and passwords. Each user of the School's electronic mail system is required to read and sign a copy of the Acceptable Use Policy prior to receiving an electronic mail account

and password. Employees are responsible for protecting the confidentiality of their account and password information.

Electronic mail access will be terminated when the employee or third party terminates their association with the School, unless other arrangements are made. The School is under no obligation to store or forward the contents of an individual's electronic mail inbox/outbox after the term of his or her employment has ceased.

Important official communications are often delivered via electronic mail. As a result, School employees with electronic mail accounts are expected to check their accounts in a consistent and timely manner so that they are aware of important announcements and updates, as well as for fulfilling business and role-oriented tasks. Employees are responsible for mailbox management, including organization and cleaning. Employees are also expected to comply with normal standards of professional and personal courtesy and conduct.

The School's electronic mail systems and services are not to be used for purposes that could be reasonably expected to cause excessive strain on systems. Individual use must not interfere with others' use and enjoyment of the School's electronic mail system and services. Employees will comply with all applicable laws, School policies, and School contracts.

The following activities are deemed inappropriate uses of the School's electronic mail systems and are prohibited:

- Use of electronic mail for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (*e.g.*, spreading of computer viruses).
- Use of electronic mail in any way that violates School policies, rules, or administrative orders.
- Viewing, copying, altering, or deletion of electronic mail accounts or files belonging to the School or another individual without authorized permission.
- Sending of unreasonably large electronic mail attachments. The total size of an individual electronic mail message sent (including attachment) should be ____ or less.
- Opening electronic mail attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.

- Sharing electronic mail account passwords with another person, or attempting to obtain another person's password. Accounts are to be used only by the registered user.
- Excessive personal use of School electronic mail resources. The School allows limited personal use for communication with family and friends, independent learning, and public services so long as it does not interfere with staff productivity, preempt any business activity, or consume more than a trivial amount of resources. The School prohibits personal use of its electronic mail systems and services for unsolicited mass mailings, non-School commercial activity, political campaigning, dissemination of chain letters, and use by non-employees.

Usage of Personal Electronic Devices

Employees are restricted in their usage of employee-owned personal electronic devices on School property and at School-sponsored events. Personal electronic devices include but are not limited to employee-owned desktop, laptop, tablet, and handheld computing devices (whether wired or wireless), USB drives, and cellular telephones.

The following activities are regulated by the Acceptable Use Policy:

- Employees are prohibited from using a camera phone (a cellular phone including a camera capable of capturing and transmitting still or full motion images) in any way that violates School policies, including illicit and illegal use.
- Employees may not use personal electronic devices or media including but not limited to CD/DVD burners and USB drives to illegally duplicate and/or distribute copyrighted materials.
- Employees may not load a bootable, alternate operating system on any School-owned computer from any employee-owned source or media.
- Employees are prohibited from using any portable wired, USB IP-telephone devices or wireless Wi-Fi IP telephone devices (such as Vonage, V-phone, or MagicJack) that can make or place calls to or from a private phone number on School networks at any time.
- Employees may not acquire, through wired or wireless connection, School-provided network or Internet access from any employee-owned computing device without the prior permission of the Campus Principal.

Disclaimer

The School shall not be liable for any employee's inappropriate use of electronic communication resources, violations of copyright restrictions, user mistakes or negligence, or costs incurred by users. The School shall not be responsible for

ensuring the accuracy or usability of any information found on the Internet/World-Wide Web.

Electronic mail transmissions, faxes, and program or data files sent, received, created, or accessed by employees are not considered confidential and may be monitored at any time by designated staff to insure appropriate use of educational and administrative technology.

The School reserves the right to restrict or terminate Internet, network, or computer access at any time for any reason. The School also reserves the right to monitor Internet, network, and computer activity in any way necessary to maintain the integrity and security of the network and the privacy and accuracy of user information.

Consequences for Violations of the Employee Acceptable Use Policy

Violations of this policy will be treated like other allegations of wrongdoing at the School. The use or installation of any software or device onto any computer or network for the purpose of controlling, collecting logins, or accessing any data or systems without written permission will result in disciplinary action. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for violations of this policy may include, but are not limited to, one or more of the following:

- Temporary or permanent revocation of access to some or all computing and networking resources and facilities.
- Disciplinary action, up to and including termination.
- Legal action according to applicable laws and contractual agreements.