DIOCESE OF
SAN JOSE

TECHNOLOGY AND USE POLICY

Effective March 1, 2020

Overview

Technology and the Internet are important resources for the Diocese to provide improved communication services to parishes and schools. The Diocese will creatively use technology and the Internet to improve services and contribute broadly to the mission of the Church. The Diocese of San Jose may provide Internet and related technology services and devices, including telephone, voice mail, computers, and mobile devices to facilitate the official work of the Diocese.

These services are provided for employees and authorized persons affiliated with the Diocese ("users") for the efficient exchange of information and the completion of assigned responsibilities consistent with the mission of the Diocese. The use of these services by users must be consistent with this policy (including all security and confidentiality provisions set forth herein).

Supervisors should work with employees to determine the appropriateness of using the Internet for professional activities and development. The various technologies are Diocesan resources and are provided as efficiency and operational tools to users who may use them for research, professional development, and work-related communications.

All Diocese of San Jose policies and procedures apply to user's conduct on the Internet and with technology, especially, but not exclusively, relating to: intellectual property, confidentiality, information dissemination, standards of conduct, misuse of Diocese of San Jose resources, anti-harassment, and information and data security.

This policy is intended to identify the principles of Acceptable Use and Unacceptable Use of the Internet and technology; define Diocese of San Jose rights; address Enforcement and Violations provisions. Employees and users granted access privileges will be required to acknowledge and sign this document.

As noted above, The Diocese of San Jose ("DSJ") may issue mobile/cellular phones, laptop/notebook/tablet computers, smart phones, and any device capable of storing corporate data and connecting to an unmanaged network and the communications services (e.g., cellular and data services) provided in support of such equipment (collectively "Devices") from time to time to designated employees to conduct business on the DSJ's behalf ("Policy"). Devices can further be defined as having the ability to receive and/or transmit voice, text, data messages and/or Internet usage without a cable connection. Every employee's Supervisor must approve of the business need for an employee to be issued a Device prior to issuance. This Policy may be amended from time to time as necessary, with or without notice.

Purpose

Devices are tools to increase effectiveness, efficiency, reduce response time and improve communication. The DSJ provides these Devices to its employees to improve communication, productivity and work efficiency, to facilitate telecommuting and remote working, working between multiple locations and to otherwise enhance the contributions of its employees. Though the DSJ expects that its employees will primarily use their Devices while working, the DSJ does understand and

acknowledge that its employees may make reasonable use of the Devices from time to time for appropriate personal use.

DSJ Business Approval:

Expenditures for Devices must follow a specific approval process, tied to demonstrated business necessity, rather than as additional compensation or otherwise. Notwithstanding prior practice, employee's personal devices shall no longer be an approved and reimbursed expense. Prior to issuance, each employee's Supervisor shall determine and approve of the employee's bona fide business need based upon the employee's job duties, budget availability and local policy, custom and practice. Convenience alone is not a criterion for issuance of a Device(s). The approval process will include a review of all aspects of the Device to ensure that each is acquired and issued at a minimum cost to the DSJ consistent with business requirements of the employee.

Principles of Acceptable Use

The use of the Diocese of San Jose's technology and Internet/Intranet access is for the work of the Diocese of San Jose and authorized purposes only. Brief and occasional personal use of the electronic mail system, the Internet or operating system add-ons is acceptable as long as, in the judgment of the supervisor and/or Technology Services, it is not excessive or inappropriate, occurs during personal, and does not result in expense, service degradation, exposure to security breaches or viruses, or loss of data to the Diocese of San Jose. Dioceses of San Jose users are required:

- To respect the work product of others. Users shall not intentionally seek information on, obtain copies of, or modify files or data maintained by other users, unless explicit permission to do so has been obtained.
- To respect copyright and license agreements for software, digital artwork, and other forms of electronic data.
- To protect data from unauthorized use or disclosure as required by state and federal laws and Diocesan regulations.
- To respect the integrity of computing systems: for example, users shall not use or develop programs that harass other users or infiltrate a computer or computing system and/or damage or alter the hardware or software components of a computer or computing system.
- To limit personal use of the facilities and equipment (e.g. printers, scanners, etc.).
- To safeguard their accounts and passwords. Accounts and passwords are normally assigned to single users and are not to be shared with any other person without authorization. Users are expected to report any observations of attempted security violations. Passwords must be provided to the Diocese.

Unacceptable Use

Unless specifically granted in this policy under Principals of Acceptable Use, any non-work use of the Diocese of San Jose's systems is expressly forbidden. It is not acceptable to use Diocesan resources, including Internet access, for activities unrelated to the mission of the Diocese, including but not limited to:

- Activities unrelated to official assignments and/or job responsibilities, except incidental personal use in compliance with this policy.
- Any illegal purpose.

- Transmitting threatening, obscene, or harassing materials or correspondence.
- Unauthorized distribution of Diocese of San Jose data and information.
- Interfering with or disrupting users, services or equipment.
- For private purposes, whether for-profit or non-profit, such as marketing or business transactions unrelated to Diocesan duties.
- For any activity related to political causes.
- Advocating religious beliefs or practices contrary to Roman Catholic teaching.
- For private advertising of products or services.
- For any activity meant to foster personal gain.
- Revealing or publicizing proprietary or confidential information.
- Representing opinions as those of the Diocese of San Jose.
- Uploading or downloading commercial software without prior authorization of the Diocese and/or in violation of its copyright.
- Intentionally interfering with the normal operation of any Diocesan Internet gateway.
- Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate Diocese of San Jose purposes.
- Violating the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way.
- Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the Diocese of San Jose's networks or systems or those of any other individual or entity.
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages.
- Sending, receiving, possessing, or accessing indecent, obscene, or pornographic materials, including child pornography.
- Failing to log off any secure, controlled-access computer or other form of electronic data system to which you are assigned; negligently exposing your computer or system to inappropriate access or use.
- Defeating or attempting to defeat security restrictions on Diocese of San Jose systems and applications.
- Downloading and/or installing unapproved software.
- Department, site or work unit specific guidelines may also apply in addition to those listed above.

Business Necessity:

DSJ business necessity occurs when one or more of these factors is present:

1. It is vital for a mobile employee to be in constant touch with the DSJ or its clients.
2. An employee is responsible for emergency preparedness and must be available and on-call around-the-clock for a specific business period.
3. A group of employees has the need for group or shared Devices such as rotating on-call contact.
4. An employee does not have access to a landline or other communication device when doing a substantial portion of his or her job and communication with a Supervisor or other DSJ employee is required.
5. The Device eliminates or reduces the need for an employee to go back and forth between one or more DSJ Work Locations and increases employee productivity.
6. Issuance of a Device constitutes the most cost-effective way to meet the business communication

requirements of an employee.

Device Selection and Service:

Diocese Technology Services, in conjunction with DSJ Finance Services, shall determine the best vendor, device, and/or service plan available, and the appropriate level of equipment to be provided, considering the features needed for an employee's approved business use. All issued devices and the data within are the property of the DSJ.

Should a Device require any hardware or software repair or maintenance it shall be completed only by Diocese Technology Services. All issued Devices will need to be returned to Diocese Technology Services from time to time to receive regular maintenance and upgrades. Timely notice will be provided when this becomes necessary.

There may also be requisite and periodic submission of issued Devices to ensure compliance with DSJ Policies in effect at that time. The DSJ also reserves the right to access, monitor, add management tools, and report any suspicious activity on any Device at any time. Please note there is no right to, and there should be no expectation of, privacy in any information created or received on any DSJ Device(s).

Employees shall maintain appropriate password protection for access to issued Devices and shall not delete or modify any security features included therein. Any unauthorized deletion of data, programs or otherwise into issued Devices by the DSJ is specifically prohibited.

Employees are not allowed to remove, alter or in any way modify any protection devices installed on any issued device(s). Any damage, data lost, or other harm to device(s) due to misuse or personal use of the employee shall be paid by the employee. Company devices are not to be shared with any one not officially working for the DSJ.

Use and Protection:

It is expected that issued Devices shall remain in the possession of the employee at all times and be functional during the employee's business day. Employees must take all necessary measures to protect issued Devices from theft or damage. If any of the former occurs, it is the employee's responsibility to report it immediately to his or her supervisor and DSJ Technology Services immediately.

Employees may be disciplined up to and including termination for non-compliance with this Policy. In addition, employees must recognize that this Policy cannot govern every operating circumstance. As such, employees must always use good judgment relative to the use, and report to the appropriate Supervisor any special or unique circumstances not encompassed by this Policy.

Employees utilizing issued Devices shall not have any expectations of privacy during the employee's work schedule. These devices contain Global Positioning Systems (GPS). During an employee's established work schedule, GPS may be utilized to locate the employee. Employees have a reasonable expectation of GPS privacy outside of his or her established work schedule. GPS will not be utilized outside of an employee's established work schedule unless there is an emergency. GPS will be used for business purposes only.

Upon termination of employment, every employee must concurrently return any issued Device(s) to his or her Supervisor. The Device(s) will then be reset, and all data deleted. There is no expectation of data retrieval by the former employee.

Personal Use of Device(s):

Provided that the employee's business need for the Device(s) is paramount, an employee's reasonable personal use thereof is not otherwise limited. However, Diocese Technology Services, every Department Head and the employee's Supervisor reserve the right to access the Device(s) and/or suspend provision of the Device(s) to the employee in the case of excessive personal use.

Device(s) shall not be used outside of a non-exempt employee's designated work schedule for work purposes. Utilization by a non-exempt employee of Device(s) outside of the employee's designated work schedule is not permitted and shall not constitute overtime unless previously authorized.

Every employee issued a Device shall be solely responsible for understanding and complying with all applicable laws and DSJ policies relating to the use thereof including, but not limited to, highway safety laws relating to cell phone usage, copyright laws, ergonomic use guidelines, privacy and security.

It is never acceptable for employees to use Diocesan technology resources, including Internet access, to transmit threatening, obscene or harassing materials or correspondence, but especially in a shared youth environment or to send, receive, possess, or access indecent, obscene, or pornographic materials, including child pornography. Such uses of Diocesan resources will never be tolerated. When warranted, law enforcement authorities will be notified.

DSJ Technology Use "Offsite"

As necessary, DSJ technology may be provided to employees hereunder for use "offsite" work purposes. DSJ technology provided hereunder must remain in employee's sole possession, custody and control at all times. Each employee shall be solely responsible for any damages that may occur to DSJ technology while it is in his/her possession, custody or control. Each employee shall be responsible for immediately reporting any loss of, damage to, or malfunctions with DSJ technology. Should any DSJ technology require repair or maintenance for damage caused while in employee's possession, custody and control it shall be completed only by DSJ. Finally, each employee shall promptly return the technology when requested by DSJ and reimburse DSJ for the value of the technology if lost, damaged, or destroyed.

Diocese of San Jose Rights

The Diocese of San Jose owns the rights to all data and files in any device, network, or other technology system used in the Diocese of San Jose. Technology Services have access to all mail and user access requests and will monitor messages as necessary to assure efficient performance and appropriate use. Messages or information relating to or in support of illegal activities will be reported to the appropriate authorities.

Users must be aware that all information stored on, entered into, or transmitted in any way through the Diocese Devices, network or technology systems, including but not limited to electronic mail messages sent and received using Diocesan equipment and voicemail messages, are not private and are subject

to viewing, downloading, inspection, release, and archiving by Diocese of San Jose officials at all times. The Diocese of San Jose has the right to inspect any and all files stored in private areas of the network or on individual computers or storage media in order to ensure compliance with policy and state and federal laws. With the exception of authorized Technology Services personnel, no employee may access another employee's Device, computer files, or electronic mail messages without prior authorization from either the employee or an appropriate Diocese of San Jose official.

- The Diocese reserves the right to log network use and monitor file server space utilization by users and assumes no responsibility or liability for files deleted due to violation of file server space allotments.
- The Diocese reserves the right to remove a user account from the network.
- The Diocese will not be responsible for any damages resulting from the use of its computers, network or information systems. This includes the loss of data resulting from delays, non-deliveries, or service interruptions caused by negligence, errors or omissions. Use of any information obtained is at the user's risk. The Diocese makes no warranties, either express or implied, with regard to software obtained from the Internet.
- The Diocese reserves the right to change its policies and rules at any time.
- The Diocese makes no warranties (expressed or implied) with respect to Internet service, and it specifically assumes no responsibilities for:
- The content of any advice or information received by a user through the Internet facilities or any costs or charges incurred as a result of seeking or accepting such advice.
- Any costs, liabilities or damages caused by the way the user chooses to use the Internet facilities.
- Any consequence of service interruptions or changes, even if these disruptions arise from circumstances under the control of the Diocese.
- The Diocesan technology resources, including Internet access, are provided on an as is, as available basis.
- Employees are individually liable for any and all damages incurred as a result of violating the Diocese of San Jose security policy, copyright, and licensing agreements.

The Diocese of San Jose has licensed the use of certain commercial software application programs for its work purposes. Third parties retain the ownership and distribution rights to such software. No employee may create, use, or distribute copies of such software that are not in compliance with the license agreements for the software and without express authorization from the Diocese.

Enforcement and Violations

This policy is intended to be illustrative of the range of acceptable and unacceptable uses of Internet facilities and is not intended to be exhaustive. Questions about specific uses related to security issues not enumerated in this policy statement and reports of specific unacceptable uses should be directed to the user's supervisor. Other questions about appropriate use should be directed to the user's supervisor. The Diocese will review alleged violations of this policy on a case-by-case basis.

When a supervisor becomes aware that an employee may have violated this policy, including but not limited to the placement on the Internet or transmission using the Internet of material that likely violates this policy or the downloading or being in possession of materials that likely violates this policy, the

following will occur:

- The Diocese of San Jose will immediately place the employee on an administrative leave pending the outcome of an investigation;

- The Office of Human Resources will notify Technology services to immediately block access system-wide to any website or database found to contain material that violates this policy;

- The Office for the Protection of Children & Vulnerable Adults will make a determination whether a forensic investigation of all Diocesan devices used by the employee is warranted.

Violations of the policy will result in disciplinary actions as appropriate, up to and including dismissal. This policy is not intended to and does not alter the at-will employment relationship between you and the Diocese. Use of Diocesan resources for illegal activity will lead to disciplinary action, up to and including dismissal and criminal prosecution. The Diocese of San Jose will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual Internet activities, e-mail use, and/or computer use.