Saint Cletus Parish

LaGrange, Illinois

Department of Information Technology

PARISH TECHNOLOGY PROCEDURES & POLICIES

February 2018 Revision

I. Introduction & Usage

Saint Cletus Parish provides and uses many forms of communication and information technologies ranging from education to business applications. These technologies, when properly used, support our business, pastoral activities, education, and enable closer and timely communication with parishioners, business associates, and the Archdiocese.

There is a continuing evolution of associated laws and conventions governing acceptable use and careless use of electronic communication tools that can have dramatic consequences, harming the parish, Archdiocese, our constituents, and our employees. These policies and procedures are intended to minimize the likelihood of such harm by educating our staff and by acting as the basis for written policies & procedures whose existence will serve to protect the parish and Archdiocese in litigation and other disputes.

The parish expects that all employees will use electronic mail and telecommunication tools and apply them daily in appropriate ways to the performance of tasks associated with their positions and assignments. Access to parish communication tools is provided in conjunction with the parish's business and staff job responsibilities. Staff use of these tools is subject to these policies and procedures as well as other Archdiocesan policies and procedures. This policy is binding for all parish staff (priests, teachers, ministers, department heads, administrators, etc. and to the extent it applies, volunteers).

Parish communication tools also may be made available to individuals who are not parish staff (i.e. consultants, vendors, committee members, volunteers, etc.). Use of these tools by such persons should be supervised by a staff person and is subject to this policy.

Definition:

"Communication tools" include, but are not limited to, e-mail, internet, computers, and phone system.

A. Acceptable Use

In the course of employment, staff may use communication tools to communicate internally with coworkers or externally with parishes, parishioners, parents / guardians, agencies, consultants, vendors, and other professional and business acquaintances. Use of telecommunications can also be used to explore educational topics, conduct research, and contact others in the educational world. Growing use of parish technologies can help keep staff on the cutting edge of practice by forming partnerships locally, across the nation, and around the world.

Policy: Personal Use

On occasion, there may be times to use communication tools for personal purposes. Personal use is strongly discouraged as it can interfere with job performance, consumes resources, gives rise to more than nominal additional costs, and can interfere with the activities of other staff members.

Policy: Personal Gain

Under no circumstances shall communication tools be used for personal gain or to solicit other for activities unrelated to parish business or in connection with political campaigns or lobbying.

Policy: Inappropriate Uses of Communication Tools

- To carry defamatory, discriminatory, or obscene material
- To infringe upon another person’s intellectual property rights (i.e. copyrights)
- Violating the terms of any applicable telecommunications license or any laws governing trans-border data flow (i.e. laws dealing with data collection, protection, privacy, confidentiality, and security)
- Attempting to penetrate computer or network security of any company or other system, or to gain unauthorized access (or attempted access) to any other person’s computer, email, or voicemail accounts or equipment: or in conjunction with the violation or attempted violation of any other law.

B. Internet Use

The parish is aware that web surfing and web browsing may be business-related and serve a legitimate function as it relates to regular work duties, but the potential for abuse exists. The internet provides access to a huge amount of information and resources that can greatly enhance our ability to deliver services to parishioners, students, and associates.

Policy: Internet Usage

The parish encourages exploration of the Internet for legitimate ministry related, job-related or professional activities, but staff shall not browse the web on parish time (for personal use), create personal “home pages” (including personal blogs and social networking except as related and approved for their ministry/department), or otherwise use parish facilities to access internet sites for reasons unrelated to parish business and job responsibilities.

Policy: Internet / Website Content

The parish may filter certain categories and websites deemed inappropriate. Some of these categories and websites may be accessed by employees with elevated privileges (for example, a teacher wishing to show an appropriate YouTube video). Regardless if the site is filtered, access to sites should be for official parish business. If you navigate to an unfiltered site or site with inappropriate content, you should exit the site and contact your immediate supervisor and/or parish IT Department.

C. Representing The Parish In Staff Postings

Any information published electronically (sometimes called a posting, wall post, tweet, etc.) is a reflection of the parish. Despite disclaimers that may be made (e.g. that views belong to a particular individual and may not reflect on those of the parish / Archdiocese), readers elsewhere may make the association between a posting and the parish and/or Archdiocese of Chicago. Staff should be aware that true anonymity is very difficult to obtain when using these tools. While chat boards, blogs, newsgroup visits, social media, and net surfing can sometimes appear to be done anonymously, accessing these services / servers through the parish’s network facilities normally leaves an “audit trail” revealing at least the identity of the parish’s proxy server and/or IP address. Inappropriate use of parish facilities may be damaging to the parish’s and Archdiocese’s reputation and could give rise to corporate and individual liabilities.

Policy: Correct Information

Staff shall make every effort to be professional in all usage of parish communication tools and ensure that information is correct before posting any articles or opinions.

Policy: Disclaimer Usage
Staff shall use a disclaimer that the opinions offered are their own and not necessary reflect the opinions or position of Saint Cletus Parish or the Archdiocese of Chicago.

D. Electronic Communication

Electronic communication tools have become extremely important means for St. Cletus to communicate with parishioners, students, parents and the general public.

While these tools are fun and exciting to use, it is important to remember that they belong to parishes and schools, and not to the individuals that may monitor and maintain them. Just like the content of a bulletin or newsletter, the messages delivered through electronic ommunication tools come from St. Cletus. Consequently, St. Cletus is responsible for these messages.

Policy: Ownership and Access of Tools for Electronic Communication
Employees may use a variety of web-based tools to communicate. These tools include, but are not limited to, websites, content-sharing sites (e.g., YouTube), social networking sites (e.g., Facebook), blogs and micro-blogs (e.g., Twitter), and other social media sites.

Employees must be sure their immediate supervisor is aware of and approves of the creation and use of any communication tools in connection with their work.

Additionally, the parish or school must “own” the website, content-sharing site/account, social networking account, blog or other social media site/account.

- In the case of a website, this means that the domain name must be registered to the parish or school, and not to any individual employee or volunteer.
- In the case of a social networking account, blog or other social media account, this means that the account is registered to the parish or school, or to a specific position (e.g., director of youth ministry) within the parish or school, and that login and password information is known to or accessible by the pastor or principal and two other employees.

Policy: Maintenance of Tools for Electronic Communication
Employees should monitor the content of any websites, content sharing sites/accounts, social networking accounts, blogs or other social media sites/accounts to be sure they do not contain any inappropriate material. Inappropriate material is content that is confidential, proprietary, pornographic, threatening, discriminatory, defamatory, disparaging, or copyright-protected.

While various employees and volunteers may work with or use these tools, designated staff members will review all content and remove inappropriate content from any and all officially authorized electronic communication tools.

St. Cletus is not obligated to host forums for public discussion on parish or school-owned tools for electronic communication. The person responsible for monitoring these tools can and should remove objectionable content.

Policy: Posting Photos, Video, and Recordings
If pictures or audio/video recordings are going to be posted online, the St. Cletus must make sure that it has obtained proper permission (i.e., written releases) before posting. Similarly, if identifying information about persons is to be posted, the St. Cletus should receive written permission from such persons before the information can be posted.

Employees and volunteers are not be permitted to post a recording of anything connected to their duties as employees or volunteers unless the parish or school has given permission for the posting and has obtained the appropriate releases.

- This rule is applicable to a wide variety of situations including, but not limited to, the following: coaches who want to post game footage; music ministers who want to post their performances at a mass or other church celebration; teachers, youth ministers or catechists who want to post footage from field trips, meetings or other events; or a sacristan who wants to post the priest's homily from the past weekend's mass.

To the extent St. Cletus can control advertising featured on officially-authorized tools for electronic communication, we will exercise good judgment in selecting advertisers and approving advertisements.

Policy: Respecting Copyright in a Digital World

Copyright laws impact St. Cletus' use of tools for electronic communication. Just because content is available on the Internet does not mean that the content can be freely used for any purpose.

- Do not post any non-original content (e.g., photographs, artwork, articles, etc.) unless and until you have obtained written permission from the copyright owner to do so.
- This guideline also extends to posting videos or recordings of masses or other events that contain performances of copyrighted music or other copyrighted material.

Responding to Negative Comments Posted on Third Party Sites

The development of collaborative web applications, like social networking sites, has created new forums for sharing information. While this is a positive development in many respects, it has also created a virtual soapbox from which individuals can air their grievances. Students and adults may want to vent frustration, post complaints or poke fun at parishes, schools, agencies, staff, students or programs online. In some cases, these communications can rise to the level of threats or bullying.

A common response is to demand that the comment(s) be removed and to take action against the person(s) posting it. However, parishes and schools have very limited control over unfavorable content posted on third-party websites or social networking sites.

- A specific site's terms of use dictate what material the site owner will remove and what will remain posted to the site.
- Often, third-party sites will only remove content that violates the law. This includes content that is defamatory, bullying, or violates intellectual property rights.
- If the individual posting the content is a parishioner or school parent, it may be more effective to ask that individual to personally remove the content.
- Please keep in mind that removal of the unfavorable content is often the most desirable outcome.

In the case of students, the extent to which disciplinary action can and should be taken will depend on the content of the information that has been posted online. Distinctions need to be made between content that is threatening, bullying or otherwise harmful to the student or others, and content that is negative but not otherwise harmful. In all cases, before taking disciplinary action, a school should consult with the Office of Catholic Schools for guidance on how to handle the situation.

E. Communicating Electronically with Minors

Electronic communication can be carried out using both physical tools such as cellular phones and webcams, and intangible tools such as email, websites, social networking sites (e.g., Facebook), content sharing sites (e.g., YouTube), blogs and microblogs (e.g., Twitter), and other social media sites.

Policy: How to Communicate With Minors

All decisions related to the means used to communicate electronically with minors should be made by a pastor, principal or social media manager, rather than an individual employee or volunteer, prior to the use of any tools.

Before communicating with minors electronically, the ministry will obtain written permission from parents to do so. Ask parents, in writing, which forms of communication they prefer be used to contact their children. Teachers, catechists, coaches, youth ministers and others should not collect student e-mail addresses and phone numbers from students; this information must be provided, in writing, by parents. In the case of young children (i.e., elementary school and middle school students), only parents should be contacted directly. In the event minors are contacted directly by employees or volunteers, parents must be copied on the content of all messages (although the duplicate message need not be sent using the same means of communication used to contact the minor).

The content of electronic communication should be brief and on topic. When communicating with a minor, write or speak as if you are also communicating with their parents; the boundaries that must be respected in oral communication extend to electronic communication. All communication must conform to Archdiocesan Safe Environment Training and the Code of Conduct. Communication that violates the Code of Conduct will not be tolerated, regardless of the medium used to convey it. Except in extraordinary circumstances, all communication between adults and minors should take place between the hours of 7:00 a.m. and 10:00 p.m. This includes the posting of content to websites and social networking sites.

The following guidelines provide specific direction for the use of certain common forms of electronic communication:

Cellular Phones/Text Messaging

- Whenever possible, use school or office lines to conduct ministry/school-related conversations.
- Except in cases of emergency, do not call minors directly (e.g., on a minor’s cellular phone). Instead, call parents’ or family lines.
- Except in extraordinary circumstances, do not share your personal cell phone number with minors.
- Do not communicate with minors individually via text message. One possible alternative to the use of traditional one-on-one text messaging is the use of social networking sites (see point one under “Social Networking Sites”).

Email

- Do not contact minors using a personal email address. Only official parish/school accounts should be used for communication.

- If possible, always copy parents on emails sent to minors. In the case of certain minors (i.e., elementary school and middle school students), only email parents.
- Do not add a minor to personal electronic mailing lists (e.g., when sending or forwarding an email unrelated to educational or ministry-based activities, do not add minors to the list of recipients).
- If you receive an inappropriate personal communication from a minor (especially a communication that is sexual in nature), keep a copy of the message and report it to your supervisor.

Social Networking Sites

- Employees or volunteers should not use personal social networking site accounts to contact minors. Instead, with permission from a supervisor, a ministry can create a group or organization page used strictly for education or ministry-related communication. These accounts must be registered to the St. Cletus using an official parish email address, instead of to individuals within an organization. All group pages or ministry/education-related accounts should be titled to reflect their official nature. Passwords to such accounts should be accessible to the pastor or principal and two other employees.
- No personal contact information should be listed in the profile fields. Only official email addresses, office phone numbers and job titles should be listed.
- Account settings should be set to maximize privacy.
- While St. Cletus is free to publicize presence on social networking sites, minors should not be sought out as contacts or “friends” (i.e., individually invited via site communication tools to associate with the group or page).
- If a minor seeks association with your personal social networking page or account, you should refuse or ignore the minor’s request (e.g., you should ignore the “friend request,” and not become “friends” with the minor).
- Do not post pictures of minors without first obtaining a signed written release from the minor’s parent(s) or guardian(s). Do not “tag” pictures of minors (i.e., label photos to increase their accessibility or visibility on a site).
- Only comment on education or ministry-related threads.
- Do not use instant messaging programs (e.g., Facebook chat) to communicate with minors.
- Official walls and pages must be frequently monitored for inappropriate posts. Inappropriate posts should be promptly removed/deleted. A specific individual should be responsible for monitoring sites and removing inappropriate content.
- If third parties create unofficial groups or fan pages about your group or organization, periodically review them for inappropriate content (e.g., unauthorized use of logos, bullying, harassing or defamatory language, etc.) You may report these pages/groups/users to the hosting site and ask that they be removed.
- All content posted by employees and volunteers must reflect Catholic teachings and values.

Specifically For Educators

Extra responsibility should be exercised in the education environment and for those who work with children. When students and parents gain access into a teacher’s network of friends and are able to view personal photos and communications, the student-teacher and parent-teacher dynamic is altered. It is important to maintain a professional relationship with students and parents to avoid relationships that could cause bias in the classroom.

- Do not accept students or parents as friends on personal social networking sites.

- Decline any student-initiated friend requests.
- Do not initiate friendships with students and parents.
- Educators should have all personal privacy settings set to “only friends.”
- Learn how “privacy” settings work.
- Limit what types of information your friends can see about you through external applications that work with Facebook.
- Do not discuss students or coworkers or publicly criticize school policies or personnel.
- Do not use commentary use commentary deemed to be defamatory, obscene, proprietary, or libelous. Exercise caution with regards to exaggeration, colorful language, guesswork, obscenity, copyrighted materials, legal consultations, and derogatory remarks or characterizations.
- Weigh whether a particular posting puts your effectiveness as a teacher at risk.
- If a staff member learns of information on the social networking site that falls under the mandatory reporting guidelines, they must report it as required by law.

F. Unacceptable Content

Although the parish generally does not monitor voicemail or electronic messages, staff should be aware that even personal email and voicemail messages may be viewed by designated parish employees without notice. Network supervision and maintenance may require review and inspection of parish communication tools.

Policy: Unacceptable Content
Under no circumstances shall any posting, voicemail, or email originating at the parish be in violation of the teachings of the Catholic Church, the letter or spirit of the Archdiocese’s Equal Employment Opportunity or Sexual Harassment policies, or the restrictions against 501c(3) tax exempt organizations. Examples of unacceptable content include, but are not limited to:

- Sexually explicit messages, images, cartoons, or jokes
- Unwelcome propositions, requests for dates, love letters, profanity, obscenity, slander, or libel
- Direct or indirect support for or opposition to any candidate for elective public office
- Distribution of campaign literature or biased voter education material
- Publication or transmission of paid political advertising, biased coverage of candidate activity or opinions that endorse or oppose a particular candidate
- Endorsements of candidates or political parties
- Ethnic, religious, or racial slurs
- Any message that could be construed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability, or religious beliefs

The standard used to determine whether or not “sexual harassment” has occurred is whether the recipient could reasonably consider the message to be offensive – the sender’s intentions are irrelevant.

G. Electronic Forgery

Electronic forgery is defined as misrepresentation of identity in any way while using electronic communication systems (i.e. by using another’s email account without permission, or by so-called IP spoofing, or by modifying another’s messages without permission).

Policy: Message Editing

Messages written by others shall be forwarded “as-is” and with no changes, except to the extent that staff clearly indicates where they have edited the original message (i.e. by using brackets [ ] or by using other characters to flag edited text).

H. Intellectual Property

Staff must always respect copyright and trademarks of third parties and their ownership claims in images, text, video and audio material, software, information and intentions. Staff may not copy, use, or transfer others’ materials without appropriate authorization.

I. Limits of Privacy

No electronic communications facility is completely secure. This means that information stored or carried over parish communication tools may be the subject of accidental or intentional interception, misdelivery, attack, or authorized parish / Archdiocese review. When stored on computers, email messages and other files typically are subject to routine back-up procedures. This means that copies of these files may be retained for long periods of time (in accordance with back-up and document retention procedures). Also, keep in mind that many site-wide backup systems do not guarantee privacy of backup copies (i.e. system administrators may have access).

Policy: Retention and Security of Messages

Email and voicemail messages, and computer-stored items (files, images, etc.) are parish property and business records, and may have legal and operational effect identical to that of traditional, hardcopy documents (for example, that are “discoverable” in litigation, and can be used in evidence). Retention of voicemail logs and email are governed by Archdiocesan Retention Schedules as outlined in the Archdiocesan Records Policy. Accordingly, all email messages shall be treated as though others may later view them. Email should NOT be considered a confidential means of the correspondence. Staff shall employ other methods of communication for documents that may contain confidential information.

Policy: Personal Information of a Minor

No user may disclose, use, or disseminate personal information regarding minors without authorization.

Policy: Supervision and Review

The parish permits limited personal use of all communications tools on the express understanding that it reserves the right (for its business purposes or as may be required by law) to review staff use, and to inspect all material created by or stored on these communication tools. Use of these tools constitutes the employee’s permission for the parish to monitor communications and to access files that are made on or with these communication tools. Reasons for inspecting files, web surfing habits, and file usage may be expected to occur in the following circumstances (which are not intended to be all-inclusive):

- Ensuring that parish systems are not being used to transmit discriminatory or offensive messages or in connection with infringement or violation of any other person’s right
- Determining the presence of illegal material or unlicensed software
- Counteracting theft or espionage
- Ensuring that communications tools are not being used for inappropriate purposes

- Responding to legal proceedings for producing electronically-stored evidence
- Locating, accessing, and retrieving information in an employee's absence
- Investigating indications of impropriety

Policy: Violations
Violations of these policies can result in responses ranging from denial of future access to termination of employment.

<u>II. Network</u>
The significance of our parish network is to provide a centralized location for files, databases, email, voicemail, security video, and other resources. By operating in a network environment, files can be better managed and backed up, resources shared, and security strengthened.

Each St. Cletus employee is designated a username and password to access network resources (files, folders, etc.). Users should safeguard this information just as they would their own personal information.

A. Username and Password
Users may access the parish network using a unique username/ID and password assigned by the Department of Technology. Users may also be instructed to establish their own username and/or password for certain resources. Network usernames/IDs usually follow first initial, last name (i.e. jdoe).

Policy: Safeguarding Your Username & Password
Under no circumstances shall it be permissible to allow another person to use one's ID or password.

B. Files & File Locations
It is important users manage files with a suitable naming convention for organizational purposes. Files should be saved to a specified network location, whether a drive or folder on a server.

Policy: File Storage
All files should be saved and stored on the specified server unless instructed otherwise. Files stored on a local computer lack security and are not generally backed up. Unless noted, files stored on a local computer can be deleted at any time without warning. (Note: Employees typically save to My Documents which is automatically re-directed to the server for back up and accessibility.)

C. Computers & Computer Usage
Computer terminals can be found in offices, classrooms, the library, technology learning center, and other strategic locations. Use of these tools is important to the education process and conducting parish business. It is important that users keep settings and features in place on these terminals for the benefit of all users. Any such changes made by the user may be reversed at anytime and without notice.

Should a user desire a special feature or setting not configured by default, the special request should be made by opening a support request with the IT Department.

Policy: Log Off
Users should log off when they leave for the day or are in a location where multiple people would be using the workstation. Shutting down is also acceptable when leaving for the day and another user is not expected to use the workstation. (Note: Shutting down will not allow employees to log on using Remote Desktop Protocol, where applicable. However, if you log off, you will still be able to access the feature.)

D. Personal Devices & Storage Devices
Personal devices are defined as computing devices (phones, desktops, laptops, netbooks, tablets, etc.) not owned by the parish and/or were not purchased through the Technology Department. Personal devices that meet specified security requirements may, at the discretion of the Technology Department, be allowed on the parish network. Personal devices may connect to alternate or guest networks and may not have access to some network resources to protect against unauthorized access.

Policy: Passwords / Screen Lock
Personal devices connecting to our local area network and/or email should be protected by a strong password and/or screen lock.

Policy: Connecting Your Personal Device
Employees who wish to connect their personal device to the network and/or email should submit their request via the Support Portal or using the support email address. IT may request specific information about the device such as security software, MAC address, operating system, etc., for consideration and audit purposes. Allowing personal devices on the network is at the discretion of the Technology Director.

Policy: Personal Device Usage
Files, data, and data usage on the personal device are the sole responsibility of the end user. It is strongly encouraged the end-user establishes a backup procedure for files and data on their personal device. The parish is not responsible for the cost of data usage on employee-owned personal devices (such as cell phone data plan usage and/or wifi charges). Any support provided by the parish IT Department for personal devices is provided "as is" with no guarantees or warranties. Repair, replacement, and extended support of the employee-owned device(s) are the sole responsibility of the employee.

Policy: Files on Personal Devices
All files created, authored, and/or modified for St. Cletus remain property of the parish. While encouraged to use local area network locations to save and store files, an employee is expected to make available any file created, authored, and/or modified for official parish use that may be located on a device outside the parish's direct control. This includes access to files saved to the "cloud". Personal devices used by employees for parish business can be subject to electronic discovery and forensic investigation.

Policy: Lost, Stolen, or Missing Personal Device
In the event a personal device configured for network use (such as email and/or wifi) is lost, stolen, or missing, the employee should immediately report this to the Technology Department. User account information (such as password) will immediately be reset.

Policy: Remote Wipe (Lost, Stolen, Missing)

In the event an email-connected device is compromised (lost, stolen, or missing), the Technology Department may execute a “remote wipe” of all data on the device. ALL DATA ON THE DEVICE/PHONE WILL BE REMOVED.

Policy: Flash/Jump Drives & Removable Media
These devices are allowed on the network at the discretion of the Technology Director and may be scanned for harmful viruses and/or malicious code. The Technology Department is not responsible for lost, stolen, or damaged drives/media. Files and data should be copied to your network folder as a backup.

E. Wireless (Wi-fi) Access

Wireless access points are located in the rectory, education building, and parish center. Mobile devices can make use of wireless connectivity for internet and network use. Employees who wish to connect their wi-fi enabled device should open a support request. (See “Connecting Your Personal Device” above.) IT will recommend a network and provide a password. IT may ask for certain device information (type of device, MAC address, etc.) to authenticate the device and approve it for network use. (Note: Devices connected to wifi may be filtered through parish security hardware.)

List of Networks / SSIDs:

- SC-WIFI – Network for devices under our direct control (encrypted - shares connections to internal servers, printers, etc.)
- SC-rectory – Network for clergy only.

Policy: Passwords
Passwords provided for secure, encrypted networks should not be shared with others unless authorized by IT (for example, a teacher may provide students with a password for the student network, if available, for a class assignment). If employees and/or guests wish to access wi-fi and do not have a password, they should connect to the guest network. Should IT find a network compromised or rogue devices on the network, the password to the network will be reset. This will require devices connected to that network be reconfigured. (Note: Wi-fi passwords may be reset with little to no advanced notice for security and integrity of user files, databases, email, etc.)

Policy: Guest Network
Our guest network is provided as a courtesy to volunteers and guests. Guests who connect to this network may be provided an acknowledgement page which indicates they are on a shared network and their data is not encrypted. Guest access is granted on acceptance of the stated term and may be denied at the discretion of the Technology Director.

F. Program Installation

A default list of programs is installed with each PC put in to service by the Department of Technology. From time to time, a user might wish to have a special program installed or demo a new program, game, or application.

Users should not load unauthorized games, applications, or programs onto a computer without first contacting the Department of Technology to evaluate security and compatibility with our systems.

Policy: Program Additions
Additional programs, games, and applications can serve as great assets to productivity, education, and business communications. Users who would like additional programs installed should open a support request.

III. Email

The parish views email as an important communication tool with staff, parents, and parishioners, vendors, and business associates. Its ease of use, availability, and low cost make it a vital connection with those we serve.

Parish employees are provided an email address for appropriate use during employment. Email addresses will be assigned and currently follow the "first initial", "last name" scheme (i.e. Jane Smith would be jsmith@stcletusparish.com).

Policy: Official Parish Email
When communicating via email for parish business, the designated employee email address should be used at all times. At no time should a personal email address be used as part of one's ministry and/or to conduct the business of the parish.

A. Email Distribution

Users should use caution when distributing their email address to websites, newsgroups, or other online solicitations without checking the website or company's privacy policy first. This will safeguard your email address from being distributed to spammers.

Policy: Protect Your Email Address
Check the website or company's privacy policy before providing your email and personal information. Avoid posting your email address on a website to prevent your address from being harvested for spamming.

B. Spam or UCE

Spam or UCE (Unsolicited Commercial Email) is unwanted email for products and services. It's the electronic equivalent of "junk mail" you might receive in your postal mailbox. Spam clogs our system and takes up employee time determining valid email versus "junk." The parish employs systems that automatically determine what email is spam, but sometimes spam messages do get through and likewise, some valid messages get flagged as spam.

Policy: Never Reply To A Spam Message Or Unsubscribe To These Messages.

Policy: Junk Email or Spam folders
Users should check their Junk Email and/or Spam folders to be sure an expected message wasn't flagged as spam (false positive).

C. Attachments

The parish views attachments as an easy way to transfer files from one party to another. This eliminates the need to fax or recreate documents already created electronically.

Employees should exercise caution at all times before opening an attachment. First, the user should determine whether or not they were expecting an attachment. Second, the user should see if they recognize the user who is sending the attachment. Third, the user should look for information in the email such as the user's signature, name, or other identifiable information which would suggest the email originated with the actual sender. Fourth, is the attachment a common file type? (.doc, .xls, .ppt, .pdf, .jpg, .gif) Malicious code, worms, or viruses can still be embedded in to these file types, but are less likely contained in these.

Policy: Opening An Attachment
Under no circumstances should a user open or download an attachment from an unfamiliar sender. Exercise care ***even from users you recognize*** as their account may have been compromised. Attachments with an extension of .zip, .bat, .exe, .vbs, etc. should never be downloaded under any circumstances without the permission of the system administrator.

D. Privacy & Security

As specified in the "Information & Usage" section, communications over email should not be considered private. Network supervision and maintenance may require review or inspection. Additionally, email sent to outside users can be forwarded, printed, or otherwise distributed without the employee's knowledge or consent. Since privacy cannot be guaranteed, special care should be given to the opinions, information, and files sent by email.

E. Checking Email From Outside Network

Users may be allowed to access their designated email account from outside the parish network. Users should visit http://mail.stcletusparish.com to access their email outside of the network. (See also item F below.)

Policy: Remote Access Security
Accessing email remotely is a convenient way to effectively communicate and stay in touch. However, no guarantees can be made of the safety and security of systems outside of the parish. When using public computers, users should make absolutely sure they log off open sessions to avoid a security breach to that user's account.

F. Connecting Your Personal Device To Email

Allowing personal devices to connect to the parish email system is at the discretion of the Technology Director.

Policy: Personal Device Password
Employees who connect their personal devices to the parish email system must password protect this device. Many applications on smart phones and tablets do not require a password once the account is established on the device. This allows anyone in possession of your devices access to your email.

(See "Personal Devices" under Section II additional information.)

IV. Voicemail and Phone System

Phone communications are vital to transacting business and communicating with parents, parishioners, and vendors.

The parish expects that employees will use the telephone and voicemail system in accordance with their positions and assignments.

A. Phone Numbers

Designated offices are provided with phone numbers, either public or private, to be used for business purposes. It is up to the department or ministry director to determine how this number will be used.

B. Outbound Calls

Calls using our phone system can be made by pressing "9" first to access an outside line.

C. Rectory 911 Calls

Outbound calls to 911 in the rectory need to dial "Memory" then "09".

D. Voicemail

Each Saint Cletus employee is provided a voice mailbox and password for official job-related use. It is their responsibility to check it often, usually daily, for new messages. Employees can opt-in for a text notification sent to their cell phone or designated email address notifying them of a new voicemail message. (Text message charges to cell phones are the employee's responsibility.)

A list of employee extensions and/or voice mailboxes is available upon request and at http://support.stcletusparish.com.

E. Checking Voicemail

Employees can check their voicemail in-house by pressing "Message" then "*#" and their 3 or 4 digit extension from any phone. A prompt for password will be heard. If a user's voicemail box is associated with physical phone, a red LED display will be flashing by the message key indicating a new voicemail has arrived. On one's own physical extension, just the message key can be selected for voicemail retrieval.

Outside of the parish facilities, voicemail can be checked at anytime by calling 708-215-5400 and pressing "#" followed by mailbox number. A prompt will be heard to enter the user's password.

F. Fax Services

Designated fax numbers may be used to send/receive facsimiles. Fax coversheets should be use for each outbound fax. Incoming faxes should have the recipient's name clearly displayed on a coversheet from the sender to distribute. (Note: It is not necessary to dial "9" first on our fax lines.)

Contact the Department of Technology or department / ministry director for a list of fax numbers.

G. TDD & TTY

Telecommunication Device for the Deaf and Telephone Typewriter features are not supported by our general phone system. If outside calls need to be made using this system, users should use the analog phone lines attached to fax machines in the rectory and school office. Dialing "9" first for an outside line on fax machines is not necessary.

V. Audio / Visual & Multimedia

The Department of Technology maintains a variety of multimedia equipment including speakers, VCRs, DVDs, laptops, LCD projectors, and other equipment which are available for use. Location of this equipment varies, but is generally strategically located based on usage and availability. Usage of this equipment can greatly enhance speakers, presentations, and video content for students, faculty, parents, and parishioners.

Policy: Checking Out Equipment

Multimedia equipment is available often on a first-come, first-served basis. For this reason, equipment should be reserved through the Department of Technology using the "Multimedia Request Form" (located at www.stcletusparish.com/forms/).

VI. Website

The parish website can play an integral part in communications with parents, parishioners, guests to parish, and even employees. The parish views a website as an important method to communicate news, information, directions, and events.

The official parish website is www.stcletusparish.com.

The official school website is www.stcletusschool.com.

A. Content Requests

Parishioners and employees can request content to be featured on the website. Turn around on such requests varies depending on complexity, but is typically two business days.

All content and requests should be sent to webinfo@stcletusparish.com. Electronic files are strongly encouraged for quicker turn around. (Common file extensions include .doc, .xls, .pdf, .jpg, .gif, etc.)

Policy: Ministries / Department heads are responsible for updating content.

Directors, coordinators, and department heads must check their web information on a regular basis to determine if content is accurate and updated.

B. Additional URLs

Saint Cletus Parish maintains the following additional URLs:

- www.stcletusparish.org – forwards to the parish home page
- www.saintcletusparish.com – forwards to the parish home page
- ~~www.stcletusserver.com – DNS resolution to our public IP address~~ (Phased out 2017/2018)

- www.stcletusparish.com – Houses the electronic help desk and ticket system
- www.cardinalcountry.org – Created for students and staff to access Google apps
- www.stcletusfallfest.com – For Fall Fest event usage

C. Facebook Pages

- https://www.facebook.com/stcletuschurch
- https://www.facebook.com/stcletusyouth
- https://www.facebook.com/stcletusschool
- https://www.facebook.com/stcletusbuilding
- https://www.facebook.com/stcletusschoolalumni/
- https://www.facebook.com/stcletusreligioused
- https://www.facebook.com/stcletusfathersclub/
- https://www.facebook.com/stcletusfallfest/

VII. Assistance & Support

The parish recognizes technical abilities vary from person to person and program to program. Tech support and training is available to employees by contacting the IT Help Desk.

A. IT Help Desk

Staffed Monday through Friday, 9am to 5pm, the IT Help Desk provides quick technical support to commonly asked questions and issues that arise from usage of our parish communication tools.

B. How to Get Help

Employees should view the Help Desk at http://support.stcletusparish.com for common questions and to submit new issues. This system includes a knowledgebase, important issues, and tracks previously submitted issues and their resolutions. New issues should be submitted using this system. A ticket will automatically be created if you send an email to support@stcletusparish.com.

The Help Desk can also be reached at extension 214 or by calling 708-215-5420.

Policy: Electronic Help Desk

Requests for support and research of issues/trouble should first go through the electronic help desk unless a system outage prevents access to the resource.

Note: Known outages and issues affecting a number of employees are indicated on our internal homepage, http://home.stcletusparish.com and on the Support Portal at http://support.stcletusparish.com.

C. Training

The Archdiocese of Chicago provides various training workshops to employees. Contact the Department of Technology for a list of these workshops.

In-house training can be provided by qualified IT personal and/or outside trainers/coaches. Submit your request to the Department of Technology for a personal training session or a staff workshop.

D. Emergency Support

The Department of Technology is available for emergency support by using the contact methods above 24/7. However, it’s the discretion of the Director of Technology and pastor as to what issues are emergency in nature.

VIII. Crisis Situations

The Technology Department can play an important role in crisis situations including but not limited to weather, power outages, evacuations, bomb threats, fire, chemical leaks or spills, crime, etc. Communication tools such as computers, phone, voicemail, and website can be critical pieces before, during, and after such events both internally (staff use) and externally (parents, parishioners, media, etc.).

Crisis scenarios vary, but might include the need for the Department of Technology to re-route communication tools (such as cable, phone, etc., in restricted / closed areas to staff which were normal locations for use of these communication tools), repair damaged communication tools in parts of the building, and safeguarding critical communication tools such as servers.

Policy: Safety & Security
First & foremost, the safety and security of those involved in a crisis situation (staff, students, parishioners, etc.) is the top priority. Directions of the School and / or Parish Crisis Team and emergency personnel for the safety & security of people take priority in any crisis situation.

A. Internal Communications / Staff Use

Communication tools such as phone, email, and website can play an important role during a crisis situation. The use of these tools during a crisis situation is dictated by the parish & school crisis plans. The Department of Technology will assist staff in using these tools during a crisis situation following the Parish and / or School Crisis Communication Plan.

B. External Communications

Communication tools can play an important role in communications with those off the parish property including parents, parishioners, media, etc. Following the Crisis Communication Plan, use of parish communication tools might be used for, but are not limited to calling parents, informing of building closures (i.e. recorded voicemail message, website posting), release of approved media information (i.e. press release via website or fax), and communications with emergency personnel.

C. Safeguarding Communication Tools

The severity of a crisis situation varies from scenario to scenario. If at all possible, communication tools should be secured to prevent from damage & theft. (i.e. If a pipe were to burst, it would be logical to move communication tools such as computers and/or servers to a different area or higher ground.) If possible, central communication and storage devices such as servers should be preserved first. These devices contain most employee files and would be the first communication tools brought into service during and following a crisis situation. These devices often contain critical communication pieces such as telephone numbers, contact names, email addresses, etc., of likely contacts in the event of a crisis situation.

D. Restoring Communication Tools

While no scenario's effect on communication tools would be the same, communication tools can be breached in emergency situations including, but not limited to power outages, fire, sabotage, and even restricted areas of the building. The Department of Technology will work the Crisis Management Team and/or emergency personnel to re-establish communications and prioritize which tools are of the most importance based on the crisis situation and resources available during the crisis.

Acknowledgment

I (the undersigned) have reviewed the Parish Technology Procedures and Policies. I understand these policies and the acceptable and unacceptable uses of St. Cletus computers, equipment, network facilities, email and mobile device syncing services provided to me. I further understand that I have no expectation of privacy in the use of these tools and systems which are subject to monitoring, inspection, records management and security policy enforcement, and that all information created, stored or transmitted via these tools and systems are the property of St. Cletus and the Archdiocese of Chicago. I understand that failure to comply with the policies and usage agreement can result in denial of access and/or disciplinary action up to and including termination.

____

Printed Name

____

Signature

_____/_____/__________
Date