THE ROMAN CATHOLIC
ARCHDIOCESE OF
ATLANTA

EMPLOYEE POLICY MANUAL

June 2023

MISSION:

We, the faithful of the Archdiocese of Atlanta, are a people of prayer, love and joy who are dedicated to the salvation of all.

As disciples and believers in our Lord and Savior Jesus Christ, we proclaim the good news and grow in faith, hope, love and service to others.

We are unified in our commitment to sacramental life, pastoral care and life-long formation in our Roman Catholic faith.

We express our love through evangelization, fellowship, Catholic education, social services and charity in the full pursuit of effective discipleship.

Any such reports will be immediately and thoroughly investigated, and preventive and/or corrective action will be taken where appropriate.

- In no case should any employee or contractor allow improper conduct to go unreported. If an employee makes a complaint of harassment or discrimination, they may be required to put those matters into written form so as to clarify the nature of the issues and to better enable the an appropriate investigation.
- If an employee makes a complaint of harassment and feels that the complaint is not being handled properly or not being investigated properly, then the employee is required to take the matter to successively-higher levels of authority.
- Employees may also utilize the services of the Archdiocesan Hotline to report sensitive workplace concerns at **1-888-437-0764.**

No Retaliation:

The Archdiocese of Atlanta prohibits and will not tolerate any coercion, intimidation, retaliation, interference or discrimination against an employee for reporting harassment, for filing a complaint of harassment, or for assisting in any investigation of a harassment claim.

4.5 GRIEVANCE POLICY

In the event an employee feels aggrieved by the action of another employee or supervisor, the process of appeal shall be that established by the Code of Canon Law of the Roman Catholic Church for the resolution of such disputes.

The employee may begin the grievance procedure with immediate supervisor. If the situation or problem is not resolved, the employee should then speak to the supervisor's supervisor, and so on up the line. Employees are encouraged to contact the Human Resources Office for further guidance on grievance matters.

4.6 COMPUTER SYSTEMS, INTERNET USAGE AND SECURITY POLICY *updated June 2023*

The purpose of this policy is to outline the acceptable use of computer equipment and technology resources at the Chancery of the Archdiocese of Atlanta (AoA). These rules are in place to protect the personnel, equipment, and reputation of the AoA. Inappropriate use exposes the AoA to risks that could affect the daily operation of the Chancery in its ability to support the administrative and ministry mission of the Chancery and parishes. This policy is to prevent the compromise of network systems and services, and the potential for legal issues. The proponent of this policy is the Office of Information Technology. Any questions or concerns should be directed to that office.

Support

- The IT helpdesk can be accessed at any time. Issues and problems should be submitted as a ticket at https://help.archatl.com

General Use and Ownership

- The "system" (which includes physical computer equipment located at the Chancery along with the network infrastructure the equipment resides on), the property of the AoA and will be used for Archdiocesan purposes only.
- Users of this system do not have a personal privacy right in any matter created on, received or sent through Archdiocesan systems. The Archdiocese, in its discretion, reserves the right to monitor and access any matter created on, received or sent from e-mail, voicemail, internet or computer systems to assure compliance with Archdiocesan policies.
- These policies apply to both physical (local) use as well as remote access to the system.
- No communication messages (e-mail, voice mail, etc.) should be created or sent that may constitute verbal abuse, harassment, slander or defamation of employees, students, parents of students, vendors, competitors or any other person or entity.
- No communication messages should be created or sent that constitute intimidating, hostile or offensive material based on race, national origin, sex, age, ancestry, physical or mental handicap or serious medical condition, disability, or any other characteristics protected by federal, state or local law.
- The Archdiocese's policies against abuse, sexual or other harassment apply fully to any and all communications (electronic or otherwise), and any violation of these policies will be grounds for discipline up to and including discharge.
- During the logon procedure, by clicking "OK" you indicate your awareness of and consent to these terms and conditions of use.
- Users will practice prudence when using their Archdiocesan computer for personal use. Personal use will be allowed during the employee's personal time, such as lunch hours and/or before and after the normal workday excluding the use of the wireless network.
- For security reasons, only AoA owned equipment will be connected to the AoA network (wired or wireless) using staff login credentials. Non-AoA owned devices would only connect to the AoA WiFi provided internet via the "CCWiFi" wireless login and passcode.
- The primary location for storing all AoA files is on the AoA network. Users are responsible for management of network directories under their purview. Each user shall review the contents of his/her directory at least once every six months to remove extraneous material.
- No personal equipment, such as printers, scanners, or other equipment is permitted to be connected to the AoA network or other AoA technology resource.
- Standard equipment configurations will not be changed.
- For security and network purposes, administrative rights are not granted to users to the local PC. The AoA Information Technology Office maintains all software, hardware, and operating system updates.
- AoA External User Policy (i.e., Contractors, Interns, Consultants, Vendors, etc.) As part of an external position with AoA, this group of individuals will be provided certain levels of access to the information technology-based systems at the Chancery. Prior to being granted this access, there are several requirements that you will need to acknowledge and agree to follow specific guidelines for Personal Equipment / Infrastructure and Safe and private computing procedures.

Internet, Email, and Document Management

- The Office of Archives and Records (ARC) has published a policy Standard Use Names of Chancery Offices and Ministries (with abbreviations). ARC lists the standard names for departments within the Chancery. Included are the various ministries run by the Archdiocese and a separate list of related corporate entities. The most current version of this list can be found here: https://archatl.com/wp-content/uploads/2020/04/arc-standard-names-offices-ministries-20230306.pdf
- All activities must be appropriate, presenting a positive, professional image of both the user and the AoA.
- Users must ensure that their conduct in public forums, email, and the Internet conforms to the teachings of the Catholic Church.
- The unauthorized use, installation, copying or distribution of copyrighted, trademarked, or patented material on the Internet is expressly prohibited.
- Users are reminded of the potential confidentiality of the message content and must use prudence before forwarding. Information is based on "need to know".
- Data leakage. Use of External Data Storage (i.e. "Free-Subscription") in the cloud such as OneDrive, Dropbox or Google Docs poses a risk to loss of control to potentially sensitive data. Its use must be strictly controlled by the AoA department heads. The only file-sharing cloud storage site that is currently approved for work use is the AoA's licensed version of Microsoft OneDrive.
- All users connected to the network have a responsibility to conserve computer resources such as bandwidth and storage capacity. The user must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-work-related uses of the Internet.
- Users or ministries requiring the mass mailing of information to parishes or individuals need to consider the use of Mail Chimp or Constant Contact (Stewardship) to prevent internal AoA internal security features from shutting down mass mailings as flooding. The use of these mail platforms can be obtained by contacting the Office of Communications.
- Users are encouraged to reduce your Outlook's clutter. Five helpful tips for you to utilize in cleaning up Outlook to make for a more enjoyable user experience. With these tips, reducing clutter from your inbox will free up space have Outlook running far more efficiently.
    - o Recognize the size of your mailbox
    - o Manage Sent Items
    - o Get Rid of Junk Emails
    - o Save Attachments to your network share drive
    - o Empty the Deleted Items folder (unless the organization is under a current litigation hold – please refer to the Office of Archives & Records for more information)
- Under the current Microsoft 365 E1 license platform, users are limited to a maximum mailbox size of 50 GB. Mailboxes are not intended to be data repositories for attached files

(Voicemail, PowerPoint, Word or Excel documents). Attachments are to be saved to your network share drive or OneDrive. AoA users will periodically review 'Sent Items' folder and 'Junk Mail' folders. New users being on-boarded are highly encouraged to attend the Archives Orientation for email management best practices.
- While on-site at the Chancery and using AoA network services, users' personal email access on our network is prohibited, but allowed on chancery Wi-Fi.
- Users email signatures are standardized by the Office of Communication and IT and follow the AoA branding code.

Remote Access

- Access: The Office of Information Technology must be contacted to set up remote access to the Archdiocese of Atlanta via your work laptop or home computer. Submit a ticket to IT. Your remote access is both password-protected and required authentication (using DUO). You will be required to enter your credentials and authenticate every time you login. This function is mandated by the auditors and the cybersecurity insurance agency and may not be disabled for security reasons.
- Personal Equipment / Infrastructure used to gain access to the Chancery systems must meet certain criteria. If not using AoA-issued equipment to gain remote access (of which there is a very limited supply), users' personal equipment will need to meet the minimum requirements. Users can use Windows based either PC's or IOS Apple computers to remotely connect to the AoA network.
- Network Drives: When working remotely, be sure to file your documents on backed-up network drives, as you would when working in the office. You should file departmental records on the M: drive. Work that is in-progress may be stored on your personal U: drive. You may use the S: drive for temporary sharing of non-confidential files across Chancery departments.
- Personal Laptops and Home Machines: Do not file work-related materials on your personal laptop or home machine's local drive, also called the C: drive. This includes your Desktop and the "Documents" folder. Only file work-related data on the network drives, once you have remotely accessed the network. Your personal laptop and home machine are not routinely backed-up by IT, and you will lose work and data if these machines become lost, damaged, or compromised.
- Email Forwarding: Do not auto-forward emails to a personal email account, or use an email account for work that is not managed by the Archdiocese. Some examples of outside email providers are Gmail, Hotmail, AOL, and Yahoo.
- Cloud Storage: The only file-sharing cloud storage site that has been approved for work use is AoA's licensed version of Microsoft OneDrive.
- If you regularly forward and store work-related documents in an unsanctioned cloud storage account, or personal email account, those accounts could potentially be subpoenaed and searched during the discovery process of a litigious event.
- Once you have completed your remote session, be sure to close down the connection by right clicking on the Windows start button (bottom left corner) and performing the following: Choose "Shut down or sign out" and "Sign out". Be sure you are performing these steps on your remote desktop session (i.e. your Chancery PC) - not on your local system and never choose "Shut down" from the second pop-up or you will shut down your

PC at the chancery and make it impossible to have another remote session without physically turning your PC back on at the office.

Security:

- KnowBe4 is the third party vendor we hire to provide the resources to:
    - Assess our user base to determine what is appropriate training,
    - Train our user base to identify the threats and use the correct response to the threats,
    - Provide unannounced internally generated Phishing tests to each user to maintain basic skills competency.
    - Chancery employees need to complete all (KnowBe4) security training offered by the IT department within the timeframe stated. Training is offered two ways: (1) as a monthly scheduled training requirement or (2) because of clicking on a KnowBe4 generated Phishing email. If user incorrectly clicks on one of these Phishes, they will automatically be enrolled in a separate additional training.
    - Noncompliance of the training requirement may result in various sanctions – up to and including dismissal. More can be found on this in the Security Awareness Training and Testing Policy.
- AOA requires complex passwords. Passwords can only be changed one time per day and a previous password cannot be used again. Passwords will expire after 180 days. It is the user's responsibility to change the password in a timely fashion as to not let it expire. Users will receive an automated email daily advising them beginning at 14 days prior to the expiration of the password. A complex password is 10+ characters in length and must contain at least three of these four types of characters:
    - Upper Case Letters
    - Lower Case Letters
    - Numbers
    - Symbols
- Various forms of multi-factor authentication (MFA) have also been incorporated into AoA's login procedure to better protect all users and their data from becoming compromised. Both Microsoft MFA and DUO authentication methods have been implemented and required to gain access to network AoA network resources.
- AoA allows access to its computing resources and requires that users identify their accounts with a username and password. Sharing user account credentials with persons other than Information Technology Staff is prohibited.
- Protect Sensitive Information. In order to secure your data, you first need to have a clear understanding of what types of sensitive information your office maintains, where it is, how it flows through the organization and who has access to it. Examples of sensitive or personally identifying information are full names, Social Security numbers, credit card and financial information, tax documents, medical records/information, driver's license numbers, passport numbers, dates of birth and email addresses. Take an inventory. Do not keep sensitive data if there is not a legitimate need for it.
- This information must not be sent through regular email. Users are encouraged to use the encrypted e-mail option from Outlook or over the phone.

- Specific action is required if a user suspects that a suspected cyber-attack has occurred. A cyber-attack is defined by the following:
    - All losses or disclosures of confidential or sensitive information,
    - All information security violations and problems,
    - All suspected information security problems, vulnerabilities, and incidents,
    - Any damage to or loss of computer hardware, software, or information that has been entrusted to their care.
- The following five steps should be followed in the case of an actual or potential information security breach:
    - Do not turn off or reboot any systems, but unplug network cables IMMEDIATELY, and/or disconnect the system(s) from the wireless network. Take notes (date; time; who discovered; what tripped the alarm);
    - Report the incident to the IT Department via ticket and phone call.
    - After confirmation from the IT staff, secure the scene. Do not allow anyone to take any action on affected systems; Preserve and protect the evidence.
    - Determine if security of sensitive data was breached and, if so, what data elements were included (e.g. name, age, DOB, SSN, medical information)
    - Follow the instructions provided by the IT staff.
- In the event the data breach includes the compromise of credentials used to access an external resource related to the operation of the Finances or Human Resources of the AoA, the following additional steps will be taken:
    - Contact the external vendor and notify them to of the potential security breach and to request they perform an audit to ascertain the extent the breach. COMMUNICATE WITH THE BANK – telephone the bank to talk through what has happened, and what actions you will be taking. If check fraud occurred, make sure you activate "positive pay" security on the bank account. If wire fraud occurred, request the bank help identify where funds were sent, and provide this information when you communicate with the Police and FBI. If some instances where rampant check fraud has occurred, you may need to close the bank account and open another one; or you may want to verify all checks that clear each day until you feel the security over the bank account is adequate.
    - Change Passwords - make sure that you immediately change your own passwords, and consider having all employees that have an account with this external resource to do so as well.
    - WRITE UP WHAT HAPPENED – to the extent you are able to, write up exactly what happened, including emails, phone calls, banking instructions and information (Number of individuals affected including numbers of AOA employees, contractors and non-AoA employees involved) . If PII has been compromised and identify by type (full name, home address, email address, social security number, passport number, driver's license number, credit card numbers , date of birth) and /or financial information. This should be a systematic summary of how the fraud or attempted fraud occurred.
    - RETAIN CORRESPONDENCE – Retain the original emails from any "imposter", which will prove helpful to your IT support group (as well as the Chancery's), the Police, and the FBI. E-Mail messages contain "header information" that can help

        pinpoint exactly where the messages originated from and prove useful to IT groups, the local authorities and the FBI
    - Additional notifications.
        - Notify local law enforcement. Contact your local Police and provide them with the narrative of what happened, and what actions you have taken so far. This will generate an official police report
        - Notify federal law enforcement. This is done by filing information at the FBI web site: https://www.ic3.gov/ . FBI Agents the archdiocese is currently working with (and may be beneficial to contact) include: Chad Hunt chunt@fbi.gov , (770) 216-3188; Jardan Smith jsmith18@fbi.gov, (770) 216-3357; or Mark Iovino maiovino@fbi.gov (770) 216-3452.
        - Immediately after the notification is made to Law enforcement, contact the Archdiocesan Communications office, the Human Resources office and the Archbishop's office in event the incident could escalate into a local media source.
- The employee must safeguard their network connection. Steps should be taken to set computer to "Locked" or "Standby" mode if the employee will be away from their computer for an extended length of time. This applies in situations when the employee is working off-site in a remote environment. The employee (as a minimum) must log off the network when leaving their computer for the workday. The best practice is to reboot your machine and allow it to be powered up in order to receive updates to the applications and operating system.
- Use Your Antivirus (AV) Tool. "Trend Micro" Antivirus (or AV) software is used to safeguard a computer from malware, including viruses, computer worms, and Trojan horses. AV software may also remove or prevent spyware and adware, along with other forms of malicious programs. Your system is presently equipped with a licensed AV agent, Trend Micro. Trend Micro™ Internet Security constantly scans your system's 'health' and blocks your computer from potentially dangerous websites and harmful files. Though it is configured to perform these functions in the background, you have the ability to review the status of the app as well as perform manual scans. Users must follow the below general practices as simple preventative measures against viruses:
    - Never open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source.
    - Delete attachments to emails that are from unknown, suspicious or untrustworthy source immediately, and then empty them from your Recycle Bin/Trash/Deleted Items folder.
    - Delete spam, chain & other junk email.
    - Never download files from unknown or suspicious sources.
    - Never forward suspicious email via email or ticketing systems with the urls enabled, in other words with all the links are still hot. Always use KNowBe4's built in Phish Alert Button (PAB) to submit a questionable e-mail to the IT department. See IT's knowledge base article for additional information.
- • USB Policy .The AoA has a policy that individual pc's will not "read" USB storage devices (including, but not limited to, thumb/flash drives, external hard drives, etc.). If users find a lost USB device, do not plug it in to identify the owner. Turn it in to the IT staff

for review. As a best practice, "Never plug unknown flash drives into your computer (work or personal).

- AoA users must ensure that the mobile computing device provided by the AoA is protected from theft or unauthorized removal at all times that the device is not in their immediate possession. AoA users are required to use the security features provided with the mobile device to prevent unauthorized access to the device. This includes ensuring that a password is set on the device. Should the device leave your control at any time (i.e. stolen, misplaced, lost, etc.), the user should report the incident to the Office of Information Technology as soon as possible.
- Violations of this policy, including breaches of confidentiality or security, may result in suspension of electronic communication privileges and disciplinary action up to and including termination and civil and criminal penalties under state and federal laws.

Administrative

- Hours of Operation / Phone Number. We provide coverage from 8 AM to 4 PM Monday through Friday. We are not staffed to remedy issues during the non-coverage times. You are encouraged to submit a ticket at this address https://help.archatl.com . IT will respond as quickly as possible on the next business day. Though the IT's main department line can be used for "true emergencies", please note that it is currently not monitored full time and the IT department may be delayed in responding to you. If you are onsite at the Chancery, it is best that you visit the IT department on the 3rd floor (North wing) in the event of an emergency.
- In an effort to better track and organize IT-related requests, we are requiring all users to begin submitting their requests into the ticketing system by following the steps below: Users can refer to communique article https://communique.archatl.com/wp-content/uploads/HelpdeskInstructions2.pdf for a complete systematic procedure or go directly to http://help.archatl.com/ and submit a ticket.
    - Submission of tickets by this method will help to better track and organize IT related requests.
    - Users should refrain from calling our hotline number directly and/or walking into our office when requiring assistance. As we try to work from a "First come, first served" basis to be most fair, these two methods of reporting a problem are reserved for emergency use only.
- AoA IT Department Red Banner Announcements. Users are encouraged to visit this site on our helpdesk page to view information related to planned or unplanned maintenance or operational events.
    - Planned: Weekly IT Maintenance Window Every Thursday: The IT Department reserves the right to perform maintenance on the network and its systems each Thursday evening between the hours of 8pm and midnight.
    - Unplanned: Typical announcements could related to email delays or technical issues related to external resources.
- Copier/Printer Support /SOS / Toner. Our third-party service contractor, Standard Office Systems (SOS), provides maintenance support and replacement toner for printers here in the Chancery. Each piece of equipment supported will have an SOS Tag affixed to the unit with a five digit number code on the tag (i.e. 28952). In order to get toner, submit a ticket

when the toner has reached end of life cycle (less than 2%). All requests for printer maintenance (streaking, blotches, alignment, etc.) will require a ticket. We will attempt to resolve and if unable, then we will place the call to SOS to have a technician make the repair onsite. Users are encouraged to visit the offices of IT (located on 3S) to pick-up needed toner during regular business hours.

- Grand Hall Use. The ground level facilities include the three Grand Halls (A, B, and C) and the smaller conference rooms known as training rooms (T10, T11 and T12). Reservations for these rooms are made through the FMX website https://archatl.gofmx.com/login to reserve the room. The Facilities Management office handles specific setups of the interior room. The IT Department, along with the Communications Department, maintains the equipment at each lectern in each Grand Hall.

4.7 Email Guidelines *updated April 2023*

Guidelines regarding the use and retention of email records are defined below and apply to all official archdiocesan email accounts for Chancery employees and Priests. When referring to Chancery employees, these guidelines exclude GRACE Scholars, the Catholic Foundation of North Georgia, and Catholic Charities.

Purpose and Scope

The archdiocesan email guidelines are intended to establish the retention and disposition requirements for   archdiocesan email records as well as the proper use of email by Chancery employees and Priests.

These guidelines apply to all emails, including copies or printouts of emails, created or received by Chancery employees (including temporary employees, contractors, and volunteers) and Priests while conducting business for or on behalf of the Archdiocese of Atlanta. Please refer to the *General Records Policy* for details regarding email as a record.

Email Retention

The Archdiocese provides for the economical and efficient management of official archdiocesan email accounts through the use of an electronic content management system (ECMS). The ECMS is administered by the Office of Archives and Records (ARC).

All email sent and received by employees is classified in the ECMS with a retention period based on an employee's department/job role. Unless specified by a litigation hold, emails are automatically deleted from employees' Outlook account after the designated retention has been met and are twice yearly destroyed within the ECMS by ARC staff. Employees are responsible for saving any emails they deem to have lasting value in a location outside of their email account. For questions about the retention of archdiocesan records, please reference the *Records Retention Schedule*.

The following email classifications have been created by the Office of Archives and Records.

Classification	*Definition*	*Retention Description*
Two Year Email	All sent and received archdiocesan emails for majority of employees and priests, unless otherwise specified.	2 years
Seven Year Email	All sent and received archdiocesan emails for a selection of employees in certain departments based on legal needs.	7 years
Twelve Year Email	All sent and received archdiocesan emails for a selection of employees in certain departments based on legal needs.	12 years
Permanent Email	All sent and received archdiocesan emails of select executives, such as the Archbishop, Auxiliary Bishops, and Chancellor.	Permanent

4.8 MEDIA COMMUNICATIONS

The Catholic Communications office works for the Archbishop to ensure that the Archdiocese of Atlanta is represented as a unified Body of Christ. We work to ensure a clear, consistent message of God's love through His Church. To ensure a consistent, unified message, all employees, contractors, parishes, schools, and institutions affiliated with the Archdiocese of Atlanta are required to comply with the following media communication policy.

- All media inquiries or contact with the media should be directed to:
    - ❖ **The Director of Communications,** *Chancery Office of Communications*
- Comments to the media can only be issued by the Communications office.
- Story submissions, letters to the editor, and advertisements to any media outlets may not be submitted without the approval of the Communications Director. The exception to this policy is the submission of information about a parish event or schedule.
- If a reporter, photographers, or videotaping crew shows up unexpectedly at your institution, contact the Director of Communications of the Chancery Office before you allow them on the grounds of your facility. You or your authorized representative may be directed to speak or not to speak with the media after the Communications Director determines if any response is appropriate.

This policy has been put in place to protect the Archdiocese of Atlanta and the people it is charged with serving.

4.9 FRAUDULENT OR DISHONEST CONDUCT & WHISTLEBLOWER POLICY

The Archdiocese of Atlanta ("Archdiocese") is committed to maintaining the highest standards of conduct and ethics. This Fraudulent or Dishonest Conduct & Whistleblower Policy ("Fraud Policy") reflects the practices and principles of behavior that support this commitment. The Archdiocese expects every employee, volunteer, officer and trustee to read and understand the Policy and its application to the performance of his or her responsibilities.