GUIDELINES FOR WORKING REMOTELY

ALL EMPLOYEES MUST FOLLOW THE ARCHDIOCESE OF ATLANTA'S EMPLOYEE POLICY MANUAL, SECTION 6.15, ON TELECOMMUTING

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 Support at https://support.archatl.com.

Your access is password protected, requiring you to enter your credentials every time you login. For security reasons, this function may not be disabled.

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 filed on your personal **U: drive**. You may use the **S: drive** for temporary sharing of non-confidential files across Chancery departments.

Laptops and Home Machines:

Do not file work-related materials on your laptop or home machine's local drive, also called the C: drive. This includes your Desktop and the "Documents" folder. File work-related data only on the network drives, once you have remotely accessed the network. Your 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.

Printing from Work Laptop:

We do not recommend connecting your home printer driver on your work laptop. We recommend printing files to your office, which you can do in a remote session. Please wait to print confidential records until you are physically back in the office. If you must print files at home, remember to follow all Archdiocesan policies and guidelines for managing records.

If you regularly print and store work-related documents in your home, your home (i.e. personal) records could potentially be subpoenaed and searched during the discovery process of a litigious event.

Cloud Storage and Email Forwarding:

Just as you would not file work-related data in a cloud storage environment at your work office, do not do this at home either. 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 cloud storage accounts are Google Drive, SharePoint, OneDrive, and Dropbox. Some examples of outside email providers are Gmail, Hotmail, AOL, and Yahoo.

The only file-sharing cloud storage site that has been approved for work use is **Dropbox for Business**. You may request access to Dropbox for Business from the Office of Information Technology, with approval of your director.

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.