THE ROMAN CATHOLIC
ARCHDIOCESE OF ATLANTA

Remote Access Requirements

As part of the offerings of the AoA IT department, remote access into the organization's network is provided to Chancery employees who would like to take advantage of working from outside of the office and have been approved to do so by their management. Prior to being granted this access, there are several requirements that you will need to acknowledge and accept:

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 following minimum requirements:

- Desktop Computer or Laptop with Windows 10. If an Apple-based desktop or laptop is being used, it must contain an operating system running on version 10.12 or later.
- The operating system on the device being used (above) is being continually updated with the latest patches distributed by Microsoft (or Apple).
- The device has at least 4GB RAM
- Ample hard drive storage available
- Internet connection speed at or greater than 25 mbps (no dial up or DSL)
- Internet/network connection MUST be secured (especially if Wi-Fi). This pertains to home as well as shared access (i.e. WiFi connection at a coffee house; airport; etc.) If connecting to a public WiFi (with a password – no open access), using a personal VPN service (such as TunnelBear or Nord) is preferred.
- A paid-version of some anti-virus application software must be loaded, in use and updated with the latest signature files.

Note: You may be asked to prove these requirements are in place at any time by producing your equipment or submitting a screenshot.

Safe and private computing procedures should be followed at all times while accessing or handling AoA-based data. These procedures include (but are not limited to) the following:

- Access will be limited only from the device or devices approved and referenced in the above section. Local passwords on the equipment should be enforced and AoA-based information should never be left on-screen while device is unattended.
- Printing of documents, if not disabled, should not be performed on printers outside of the Chancery.
- Personal e-mail accounts (i.e. Gmail; Hotmail, etc.) are never to be used to disseminate AoA-based data or information. Only archatl.com based e-mails should be used.

Note: The use of personal email accounts could potentially be subpoenaed and searched during the discovery process of a litigious event.

Created March 2020

2401 Lake Park Drive, S.E. • Smyrna, Georgia 30080-8862
main: 404-920-7800 • fax: 404-920-7801 • archatl.com