Policy on Use of Smart Phones and Tablet Devices

A smartphone is a cell phone that offers more advanced computing ability and connectivity including over-the-air Internet access and email syncing. Smartphones may be thought of as handheld computers with integrated mobile phone capabilities and Internet access. Smartphone operating systems provide a platform for application developers to develop and distribute 3rd party applications on the device. Thus, they combine the functions of a cell phone, camera and personal digital assistant (PDA) for email calendar and contacts syncing with email and other applications (apps) on the device. Tablets also offer similar functionality but typically do not include cell phone calling capabilities.

Growth in demand and use of advanced mobile devices boasting powerful processors, abundant memory, larger screens, and apps has outpaced the rest of the cell phone market for several years. Smart devices are important tools in today's highly mobile workforce.

Such devices pose a risk to Archdiocesan data security due to their ability to be used as a data storage device allowing confidential data to be synced or copied from AOC information stores and possibly stolen or lost.

Significant costs can be associated with these devices including IT support costs, cellular contract compliance management costs, costs of provisioning AOC syncing services, the purchase cost of the devices, warranty and insurance costs, and the monthly recurring data service fees that are incurred to allow wireless access to internet for mail synchronization and web browsing when WiFi is not available.

Policy: Smart devices and services that are contracted in the name of an Archdiocesan Agency/Parish/School or paid for by those entities must be approved in advance by the Department Director, Pastor or Principal.

Procedure

Archdiocesan Agency/Parish/School contracted units are to be on the Archdiocesan Master Contracts with the wireless service providers whenever possible to obtain the most favorable terms and pricing.

Policy: Smart devices that are purchased with Archdiocesan Agency/Parish/School funds or for which the service is paid by those entities, must be used primarily to conduct the business or ministry of said entities.

Policy: Authorized smart device users must use a pin or other biometric, or hardware provided means, to secure the device to preclude unauthorized access.

Policy: Syncing services with the AOC email system must be authorized by the user's Director, Pastor, or Principal due to cost and data security considerations. Smart device users authorized to sync with the Archdiocesan corporate email systems have additional duties to safeguard Archdiocesan information resident on the phone by adhering to prescribed security procedures and safeguards and to such ends, users are to have no expectation of privacy. AOC syncing users are only to download applications from authorized sources. Only devices and operating configurations approved and supported by IT may be used.

Procedure

Smart device users will follow required procedures to obtain authorization from their Director, Principal or Pastor prior to a request to IT for mail syncing services. A condition of use includes following the published acceptable usage practices and policies including those regarding setup, synchronization, device management, notification procedures upon loss of device or termination of employment and device operation. Such procedures are established by the Office of Information Technology and are updated as needs, changing technology or risks require. Details are available on the IT website at http://it.archchicago.org.

In the event of a lost device, change in devices, or change in employment the user is to advise IT immediately. In those circumstances, or if there is an identified risk to AOC data resident on a device, a remote erasure of all data on the device will be initiated remotely by the Office of Information Technology, and may be done without notice. Users are responsible for advising the Office of Information Technology of the loss or breach of their authorized device. Users are responsible for backing up any information on the device outside of corporate email, corporate contacts, and corporate calendar and further agree to hold the Archdiocese harmless in the event of loss of personal information, applications or data stored on the device.

Some mobile device apps can contain hidden tracking information, sleeper viruses or other malware. Applications are only to be downloaded from authorized sources. Consult the IT website at http://it.archchicago.org for details and the latest information concerning supported configurations.

Policy: Archdiocesan employees/volunteers/clerics may not sync devices that are not owned and provided the Archdiocese or properly authorized with the Archdiocesan email/calendar applications. Personally owned devices may access the Archdiocesan email system using the mobile device Internet browser via the system's standard interface or the simple web access interface via the portal.