403 Other Rules And Restrictions

403 OTHER RULES AND RESTRICTIONS

403.1 Ownership:

All Archdiocesan procured software and hardware, including Smart Phones, are the sole property of the Archdiocese.

403.2 Unapproved Software:

Employees may only install approved software on Archdiocesan Smart Phones.

403.3 Compliance with IT Policies:

Smart Phone users must read and follow the Division of Information Technology's Computer Use and Internet Policy, available here and Mobile Device Security Awareness and Usage Guidelines, available here.

403.4 Password Protection:

Employees must, at a minimum, enable 4-digit password protection within the Smart Phone. It is the sole responsibility of the employee to remember the password. Employees may not disable password protection or enable automatic remembering of passwords.

403.5 Personal Smart Phones:

Employees may not connect their personal Smart Phones to the Archdiocese's computers or network.

403.6 Sensitive Information:

Employees should not store sensitive or confidential Archdiocesan

information (including files or documents) on Smart Phones.

403.7 Repairs:

The Division of Information Technology should be contacted if a Smart Phone requires repair. Smart Phones will not be sent for repair until all user/Archdiocesan information is removed.