RCAB ELECTRONIC USE POLICY

Effective: July 1, 2017

Abstract

This document provides guidelines for the use of information technology resources at the Roman Catholic Archbishop of Boston, a Corporation Sole.

The RCAB Information Technology Department

Contents

STATEMENT

This policy sets out guidelines, processes and expectations for use of information technology resources, including, without limitation, computers and information systems, networks, data, the internet, and all modes of electronic transmission and communication.

APPLICABILITY

This policy applies to all RCAB staff members, volunteers, interns, contractors, vendors and visitors.

This policy applies to all RCAB offices and locations that utilize RCAB information technology resources. This includes the Pastoral Center, related entities that are located at the Pastoral Center and all remote locations that utilize RCAB information technology resources, e.g., Pregnancy Help, etc.

This policy does not apply to those related entities located at the Pastoral Center that have an established network environment separate and logically distinct from the RCAB network which they manage and administer themselves.

This policy does not apply to local parishes. Parishes are strongly encouraged to use this policy to help develop their own electronic use policy.

RCAB reserves the right, within its sole discretion, to limit or deny access to RCAB Systems.

Any violation of the RCAB Electronic Use Policy ("this policy") by staff or interns is grounds for discipline up to and including termination of employment or other appropriate penalties.

Any violation of this policy by contractors or vendors may be deemed to be a breach of contractual arrangements.

Any violation of this policy by volunteers or visitors is grounds for the immediate removal of access to all RCAB Systems and information technology resources, including, without limitation, internet access.

TERMINOLOGY

"RCAB" – refers to Roman Catholic Archbishop of Boston, a Corporation Sole.

"RCAB Systems" - refers to all systems, services, networks, devices (including, without limitation, servers, desktop computers, laptops, tablets, cellular phones, and telephones, and Voice over IP phones), email, internet access, file storage (including, without limitation, network storage and portable storage devices such as USB thumb and other drives) owned, leased, licensed or managed by RCAB.

"User or Users" – refers to anyone using RCAB Systems.

"Data" – refers to all electronically transmitted or stored data or information, including, without limitation, documents, databases, voice mails, text messages, emails and their attachments, videos, sound files, graphic and geographic spatial data files.   Data also includes, without limitation, software and programs designed to operate on any RCAB Systems, including, mobile devices.

"Software" – is a general term referring to computer programs and applications designed to be installed on computers or mobile devices with the express purpose of supporting an activity. Examples include business applications such as Microsoft Word or Adobe Reader, etc. Software need not have a user interface with which a User interacts with the software but may run "in the background".

"Unauthorized equipment" – refers to any equipment, including, without limitation, desktop computers, laptops, routers, switches, wireless access points (Wi-Fi), external hard-drives, NAS Drives, etc., that has not been purchased or authorized by RCAB's IT Department (the "IT Department"). It also refers to any other equipment that has not been explicitly approved by the IT Department to operate on the RCAB Systems.

"Hacking" – refers to using a computer to gain unauthorized access to Data or computer resources.

GENERAL POLICIES AND GUIDELINES

Ownership

All RCAB Systems and Data are the property of the RCAB and are provided to staff and other Users to help facilitate the work of the RCAB. Neither the Data nor the RCAB Systems are the private property of any User. RCAB reserves the right to monitor and physically inspect all or any part of the RCAB Systems at any time, without notice to an affected User.

Monitoring

RCAB Systems monitoring may include, among other activities:

- Monitoring which websites Users visit,
- Reviewing materials and Data uploaded or downloaded by Users to the internet or to Office 365 accounts, box accounts, etc.,
- Reviewing email sent and received by Users.

Sexual or Other Harassment

RCAB policies against sexual harassment or any other form of harassment, including, without limitation, the RCAB equal opportunity policy, apply fully to all RCAB Systems and Data. Any violation of those policies is grounds for discipline up to and including termination of employment or other appropriate penalties.

- No Data may be created, stored, or transmitted if it contains fraudulent, harassing, intimidating, hostile, or offensive material concerning race, color, religion, sex, age, national origin, disability or any other classification protected by law.

- Any Data or information received that is deemed to be fraudulent, harassing, intimidating, hostile, or offensive concerning race, color, religion, sex, gender, age, national origin, disability or any other classification protected by law should be deleted. If receipt of such types of information persists, this should be reported to the Director of IT.
- Any violations of this policy should be reported immediately to the Director of Human Resources.

Copyrighted Materials

RCAB Systems shall not be used to copy, store, send or receive copyrighted materials or Data, trade secrets, proprietary information, or similar third party materials without prior authorization from the owner of such materials. If uncertain about whether Data is copyrighted, proprietary, or otherwise inappropriate for transfer, a User should resolve all doubts in favor of not transferring the information and consult the Office of General Counsel (OGC).

- Users are responsible for complying with copyright law and applicable license agreements that may apply to Data and to any systems on which that Data is utilized.
- No User may agree to a license or download any Data for which a fee is charged without first obtaining the written permission from the Director of IT.

Solicitation

RCAB Systems may not be used to solicit for political causes, commercial enterprises, outside organizations, personal fund raising, personal reasons, or other non-job related solicitations.

Professionalism

Users must conduct themselves in a courteous and professional manner when utilizing RCAB Systems. All Data and communications are to exhibit Catholic values of faith, service, and integrity. Please note that Data, including, without limitation, contents of emails and documents, are highly transportable and may be accessed and read by unintended recipients.

EMAIL

Every User with an RCAB email address is responsible for using the email system properly and in accordance with this policy.

- The email system and all emails and attachments sent, received, or stored (whether locally or elsewhere) are the property of RCAB.
- Use of the RCAB email system for personal purposes is not permitted. The RCAB email system is for business purposes only.
- RCAB business email should not be forwarded to personal email accounts or any nonRCAB systems without permission from a department head, except in the ordinary course of performing duties on behalf of RCAB.

- RCAB business email should not be forwarded in bulk to personal email accounts or any non-RCAB systems without permission from a department head.
- Users have no right of personal privacy in their use of the email system. Use of a User password does not create any rights to privacy.
- RCAB may monitor, access, retrieve, and delete any Data created, stored, sent or received over the email system, for any reason and without the permission of any User.
- RCAB reserves the right to change User passwords for any reason to enable account access.
- Even though RCAB has the right to retrieve and read any email messages, those messages should still be treated as confidential by other staff members and handled accordingly. Staff members are not authorized to retrieve, read, forward, or print any e-mail messages that are not intended to be sent to them. If a staff member inadvertently or incorrectly receives an email message that he or she was not intended to receive, please contact the sender to alert him or her of the error and delete the email.
- To ensure optimal systems performance and to minimize maintenance costs, Users should delete outdated or unnecessary emails and computer files in compliance with any applicable document or data retention policies.
- All staff members should include contact information on the bottom of each e-mail sent, including e-mail address, street address, job title and direct dial telephone number.

Microsoft Office 365

Every User with an RCAB Office 365 account is responsible for using the system properly and in accordance with this policy.

The Microsoft Office 365 system is administered and managed by the RCAB and is considered one of the RCAB Systems. All acceptable use policies explicitly noted in this policy, including, without limitation, those listed in the section on 'Email' apply equally to the use of the RCAB Office 365 system.

PASSWORDS

Users are expected to protect passwords used to access RCAB Systems.

Users are not to keep passwords in a manner where others are able to readily see or access them. This includes on sticky notes, under keyboards, etc. Passwords should not be shared.

Users should lock their computer (CTRL-ALT-DEL) when stepping away from their desks.

The Pastoral Center, and other related locations, host visitors, groups, as well as other facility maintenance personnel, etc., so due diligence in protecting access to RCAB Systems is expected of all Users.

INTERNET ACCESS

Access to the internet is provided to all staff for the express purpose of accomplishing job tasks and responsibilities.

- Use of the internet for non-business purposes is limited to *de minimus* use only.
- Use of the internet to access personal webmail including Hotmail, Outlook, Gmail, iCloud, Yahoo, Verizon, Comcast, etc., is not permitted.
- Personal email should only be done on personally owned devices such as smartphones or tablets utilizing the RCAB_Guest Wi-Fi only.
- Computer resources should not be wasted. Examples of waste include:
    - Playing computer games, o Streaming non-work related videos, e.g., YouTube or audio files, e.g., Pandora, o Unnecessary printing.
- User's personal Data, including, without limitation, documents, photographs and videos, should not be stored on any RCAB Systems.
- Posting of Data on the internet requires approval from the Head of your Department. Once approved posted Data should:
    - Contain all proper copyright and trademark consents and include required notices, as appropriate.
    - Comply with all applicable laws.
- RCAB may use software to help block inappropriate websites. Nonetheless, RCAB cannot protect Users against the existence or receipt of material that may be offensive to them. If a User encounters inappropriate material he/she should immediately close the site and report the incident to the IT Service Desk (extension 5678).
- RCAB may impose stricter internet filtering policies at any time without notice.

VIRUS DETECTION

Files obtained from sources outside RCAB, including, without limitation, files brought from home; files downloaded from the internet; files attached to emails; and files provided by contractors or vendors, may contain malicious viruses that could cause significant damage to RCAB Systems.

- Users should not download files from the internet, open email attachments from unknown senders, or use storage devices from non-Archdiocesan sources, without first scanning the material with IT-approved virus checking software.
- Users should familiarize themselves with best practices for handling emails from unknown sources or when browsing the internet. Clicking on a suspect link may open the door to a computer virus that could quickly spread and damage the network.

- If a User suspects that a virus has been introduced into the network, he/she must notify the IT Service Desk immediately.
- For help with virus scanning please contact the IT Service Desk.

A Special note on Thumb Drives

Thumb drives (USB memory sticks or flash drives) are notorious for transmitting viruses.

- Only RCAB IT Department provided thumb drives should be used on RCAB systems.
- Use all thumb drives only with extreme care and due caution and ideally not at all.
- Do not use thumb drives provided by non-RCAB sources including, without limitation, those picked up at conferences and vendor exhibits.
- Do not plug in any “found” USB drives just to see what is on them – hand these in to the Service Desk.
- Do not open any files on an RCAB provided thumb drive without first scanning the drive with an IT-approved virus checking software.

UNAUTHORIZED HARDWARE

IT provides all necessary computer equipment to Pastoral Center staff members and other Users. No User is authorized to use equipment purchased through an outside vendor without first consulting with IT, nor is any User permitted to connect unauthorized equipment (see definition above) to the RCAB network either at the Pastoral Center or at remote office locations.

At this time RCAB does not support Bring Your Own Device (BYOD), which means that personal computers or other computing devices purchased by individuals, departments, or related entities, cannot be connected to the RCAB network.

Notwithstanding the foregoing, under very limited conditions, stringent controls, and prior written approval from the Director of IT, some non-RCAB devices may connect to the RCAB network. In these cases the RCAB IT Department will install various software on the device and the User will need to agree to allow RCAB IT to completely wipe the contents of the device as and when deemed necessary and without the User’s prior approval. This may result in personal Data or programs being lost and unrecoverable.

Apple Devices

To ensure that all devices on the RCAB network can be effectively managed, patched, updated and secured, the RCAB IT Department can no longer support Apple devices. Apple devices fail to meet the criteria for security, maintenance and control needed to keep RCAB Systems and Data safe and so are not authorized to join the RCAB Network.

The following devices will no longer be joined to the RCAB network: MacBook (Macbook, Macbook Air, Macbook Pro), iMac, Mac Pro, and Mac Mini. This applies regardless of how the equipment may be purchased.

Existing Apple devices will be grandfathered in until either:

- they are end of life and need replacement – at which time they will be replaced with a Windows device;
- they are replaced as part of a general desktop device refresh;
- the IT Department deems that the Apple device needs to come off the network.

Special arrangements may be made for those individuals that require the advanced graphics authoring that Mac's provide. In this case, prior approval from IT will be required as well as 'obligations of use' agreed to.

The RCAB IT Department will continue to purchase and support Apple iPads and iPhones.

A Special note for Visitors

Visitors, contractors, vendors and other non-RCAB staff are not permitted to "unplug" any RCAB devices or "plug-in" any non-RCAB devices to Ethernet jacks located in any of the RCAB offices and facilities.

Visitors, contractors, and vendors needing to "plug-in" to an Ethernet jack are required to contact the IT Service Desk before doing so to obtain permission. Note that computers, laptops and other hardware may be inspected or scanned. This does not guarantee that permission will be provided.

Visitors to the Pastoral Center are welcome to use the "guest" wireless network, "RCAB_Guest". This resource is provided as a service and can be utilized at the User's risk. RCAB assumes no responsibility for any damage that may directly or indirectly occur to any hardware, software, or Data when using this service.

The RCAB IT Department makes every effort to provide comprehensive, high quality guest WiFi. However, there is no guarantee of availability or dependability, especially when hosting very large groups of visitors.

It is the responsibility of the group or department hosting the visitor, contractor, or vendor to ensure compliance. Any questions or concerns can be directed to the IT Service Desk.

UNAUTHORIZED SOFTWARE AND APPLICATIONS

Software downloaded from the internet and installed on computers may cause significant damage to computers and may quickly infect a network. Viruses, malware, and tools designed to steal Data can inadvertently be introduced and create problems impacting all Users. This can occur even if the software appears to be from a reputable vendor or website. Because of this risk, Users do not have the permission to install software on network attached computers and laptops. The IT Service Desk maintains an inventory of approved software than can be requested and installed. To do so submit a ticket through the IT support portal (https://ithelp.rcab.org).

At times a group or department may require software that is specific to their business need and may need to install and evaluate several solutions before selecting one. In this case the IT Service Desk will furnish an appropriate test environment where the software evaluation can be completed and the security implications assessed by the IT Department. With IT approval, the software can then be added to the approved software inventory and made available for deployment to computers.

Software not in the approved software inventory is deemed to be unauthorized.

UNAUTHORIZED USE

Users are expressly prohibited from pirating software, stealing passwords, Hacking other computers, either local to the network or not, attempting to gain access to files, folders, computer resources, including firewalls, network equipment and servers, to which access has not been provided as part of their daily duties or access expressly approved, bulk emailing not in accordance with User's job responsibilities, or any unlawful activities or those not in accordance with the acceptable use policy.

CONFIDENTIALITY

All RCAB Data relating to the Pastoral Center and/or the RCAB is considered confidential. Therefore, Users must treat all matters accordingly.

- No RCAB Data may be removed, copied or forwarded to any non-RCAB system without permission from a department head, except in the ordinary course of performing duties on behalf of RCAB.
- No RCAB Data may be forwarded or disclosed to anyone, except where required for an authorized purpose.
- Users may not disclose any confidential information, purposefully or inadvertently through casual conversation, to any unauthorized person inside or outside RCAB.
- Staff members who are unsure about the confidential nature of specific information should ask a department head for clarification.

PERSONAL INFORMATION

Although all Data are considered confidential unless otherwise defined, some Data are considered to be Personal Information and are protected by law. Special care needs to be taken when handling or storing Personal Information.

Personal Information or "PI" comprises an individual's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such person:

(a) Social Security number;

(b) driver's license number or state-issued identification card number; or

(c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal Information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Without limiting the definitions noted above, if you have access to, see, or work with PI you are required to follow the Personal Information Security Policy (effective February 16, 2010). Copies of this policy are available from the Human Resources Department.

BACKUPS

The RCAB IT Department utilizes backups to ensure that business documents and files are not lost due to a significant IT event or mishap. All files stored on the H: or I: or R: drives are routinely backed up and sent off-site for safe keeping. The following devices are **NOT** backed up and should they malfunction or be subject to a virus, files stored on these devices would not be recoverable:

- Desktop computer drives such as the C: or D: drives or internal Apple device drives;
- Laptops, tablets, or other mobile devices;
- Departmental Network Attached Storage (NAS) or other external storage devices; and

□ Box accounts, OneDrive accounts, or other cloud storage solutions.

All business documents and files should be stored on the H: or I: or R: drives to ensure they are included in nightly backups.

In certain situations virus infected devices will be wiped in their entirety, meaning that all information stored on the device will be unrecoverable.

LOST OR STOLEN DEVICES

If any RCAB device, including a desktop, laptop, tablet, mobile device, or any other device owned or managed by the RCAB IT Department is lost or stolen, this needs to be reported immediately to the Director of IT and the Risk Management Office.

QUESTIONS

Any questions about this policy should be addressed to Human Resources Department.

DOCUMENT HISTORY

Version	Date	Author	Description
1.0	06/15/2009	IT, unknown	June 2009 version.
2.9	06/01/2017	IT, Peter Bujwid	June 2017 version. (v2.9)

USER ACKNOWLEDGEMENT

I acknowledge that I have received, read, and understand the RCAB Electronic Use Policy. I understand that the RCAB has the right to change these policies from time to time. I acknowledge that at times the IT Department may test policy compliance and understanding without notice. I also understand and agree that any violation of these policies may lead to disciplinary action, up to and including termination of employment by the RCAB or loss of business relationships with the RCAB, with or without notice.

☐ I am an employee, intern, or volunteer, working for the RCAB.

☐ I am a contractor or vendor working for the RCAB (also complete section 2)

____
Signature

____
Name (please print)

____
Date

Section 2: This section is for vendors, contractors, and visitors:

____
Name of Company or Affiliation

____________________________ ____________________________
Address Phone Number

Signed User acknowledgements should be returned to the Human Resources Department.