Catholic Diocese of Brownsville

Information Technology

Policies and Procedures

July, 2019

TABLE OF CONTENTS

Contents

1 Introduction

This document has been developed by the Information Technology Department in order to familiarize Diocesan employees with Catholic Diocese of Brownsville (CDOB) Technology and provide information about working conditions, key policies, procedures, and benefits affecting employment at CDOB.

This guide was developed to help employees of the Catholic Diocese of Brownsville by answering common questions concerning technology available at the Catholic Diocese of Brownsville.

The Information Technology Department supports the Brownsville Chancery Building, San Juan Pastoral Center, Parishes, Catholic Schools, La Merced / El Rosario Homes, Catholic Charities and other Diocesan affiliates.

The IT department also manages the CDOB website (www.cdob.org), Office 365 Systems for CDOB Employees including Main Offices, Parishes and Schools and Google Apps for Schools.

Please assist us in keeping this document current and correct. If you find any information that needs updating, please contact the Help Desk at helpdesk@cdob.org

In addition, we invite and encourage your feedback. Future revisions will incorporate your suggestions or ideas for improvement.

1.1 Changes in Policy

This manual supersedes all previous IT employee manuals and memos.

While every effort is made to keep the contents of this document current, Catholic Diocese of Brownsville at its option, may change, delete, suspend or discontinue parts or the policy in its entirety, at any time without prior notice. In the event of a policy change, employees will be notified. Any such action shall apply to existing as well as to future employees.

Version 2.0	3/25/2015	
Version 2.1	4/14/2015	Email Archive System Update
Version 2.2	9/01/2016	Help Desk, Technology Standards Updates
Version 2.3	3/26/2018	Sensitive Data Policies, Technology Standards, Multi-Factor Authentication for Office 365 and Website

Version 2.4	7/12/19	Contact Information, Software

1.2 Purpose

The purpose of this document is to outline appropriate and inappropriate use of Diocesan Information Technology; which constitutes an expensive and valuable resource. Employees have a responsibility to use these resources in an efficient, ethical and lawful manner. The Catholic Diocese of Brownsville has a right and a duty to protect its valuable Information Technology resources and to define the proper uses for said equipment.

1.3 Scope

These procedures and policies are for all employees of the Catholic Diocese of Brownsville at the Chancery, San Juan Pastoral Center, Catholic Charities, Newman Centers and La Merced and El Rosario Homes who have or are responsible for a “CDOB computer account”, or any form of access that supports or requires a password, on any system managed by the IT Department, and or have access to the following equipment:

Stand Alone PCs, Mobile Devices, Copiers, Facsimiles, Telephone Systems, Mail Processing Machines and Time-Clocks. For all other Diocesan entities like Parishes, Schools, etc. this document serves as a guide and to describe our services and responsibilities.

2 Service Level Agreement

The IT department is committed to respond to every request for assistance in a timely manner. The IT department has created this document to provide information to Diocesan users on the types of issues we can assist with, the expected response times and the different ways in which requests can be submitted.

2.1 Response Times

Help Desk tickets placed between 8 AM and 5 PM Monday thru Friday will be responded to within the following time frames. For Help Desk Tickets received outside normal working hours please see 4.2 After Hours Emergencies.

RESPONSE TIMES	**Business Hours**
Phone or Remote Assistance	8 Business hours
Desk side Assistance	16 Business hours

2.2 After Hours Emergencies

An emergency is defined as an event or issue with widespread impact. A single individual’s inability to perform a required action may not be classified as an emergency and will be addressed during normal business hours.

In the event of an emergency please contact the Help Desk at:

(956) 592-2878 or (956) 698-9754

The IT Department does not have a dedicated Staff to cover after hours calls, we will do our best to take care of emergencies.

2.3 Help Desk Tickets Priorities

All requests for assistance by the Help Desk are prioritized to ensure that issues are dealt with in the most appropriate order.

SEVERITY	Definition
Urgent	All users are affected (e.g. Internet, network connectivity etc.)
High Priority	All users are affected (limited work allowed)
Medium Priority	Select users are affected (no work allowed)
Low Priority	Select users are affected (e.g. printer install, passwords etc.)
Question	Functional question – How to accomplish a task

2.4 Issue Resolution

It is the goal of the Information Technology department to resolve each issue as quickly as possible. We will strive to resolve each issue to the requestor's satisfaction within two (2) business days of submission. Some issues may require more work and planning and will be reclassified as projects with their own timelines. The requestors will be notified of reclassified projects within two business days of submission.

2.5 Statement of Support

The Help Desk will support only hardware and software owned by the Diocese of Brownsville or affiliate (unless an agreement in place). Software and hardware should not be installed without previously contacting the IT department. Any unapproved software or hardware will not be supported and may be removed.

3 Information Technology Department

The Information Technology Department is located in the following locations;

Chancery Building
1910 University Blvd.
Brownsville, Texas 78520

San Juan Pastoral Center
700 Virgen de San Juan Boulevard
San Juan, Texas 78589

3.1 Staff

Alberto Zavala, MCSA, Information Technology Director
azavala@cdob.org
956-550-1540 - Brownsville Office
956-784-5005 - San Juan Office
956-698-9754 - Mobile
956-542-6751 - Fax

Leonardo Mendez, IT Specialist, Lower Valley
lmendez@cdob.org
956-550-1547 - Brownsville Office
956-592-2878 - Mobile

Jaime Martinez, IT Specialist, Upper Valley
jaime.martinez@cdob.org
956-784-5004 - San Juan Office

4 Help Desk

4.1 Help Desk Contact Information

The Help Desk is staffed Monday through Friday from 8 AM – 5 PM. The Help Desk serves as a single point of contact for Diocesan users with IT issues. A Help Desk ticket is required in order to be serviced. Please do not call or email any IT Staff member directly unless you cannot get access to the Help Desk System or send emails to helpdesk@cdob.org
Help Desk tickets will take precedence over phone calls, texts or emails addressed to I.T. Staff individually.

Some of the advantages of creating a ticket in our Help Desk System include:

- User has a standard way of reporting helpdesk issues.
- User builds a helpdesk history that will help establish and identify problem areas.
- User can have confidence that each issue has been logged and is being dealt with.
- User should receive better service, and have issues resolved in a timely manner.
- User will receive automatic email notification about status of their helpdesk ticket.

Following are the available options at this time to create a Help Desk Ticket:

- **Web:** By using our Help Desk Portal at: http://helpdesk.cdob.org
- **Email:** By sending an email to: helpdesk@cdob.org

  Please Include:
    - Description of the Problem
    - Location: Parish, School, Office
    - Phone Number

- **Phone** (Only if Web and Email are not available)
  Help Desk Main Number: **(956) 550-1500 or Ext. 300**

  Leonardo Mendez, IT Specialist, Lower Valley
  956-550-1547 – Office | 956-592-2878 - Mobile

  Jaime Martinez, IT Specialist, Upper Valley
  956-784-5004 – Office

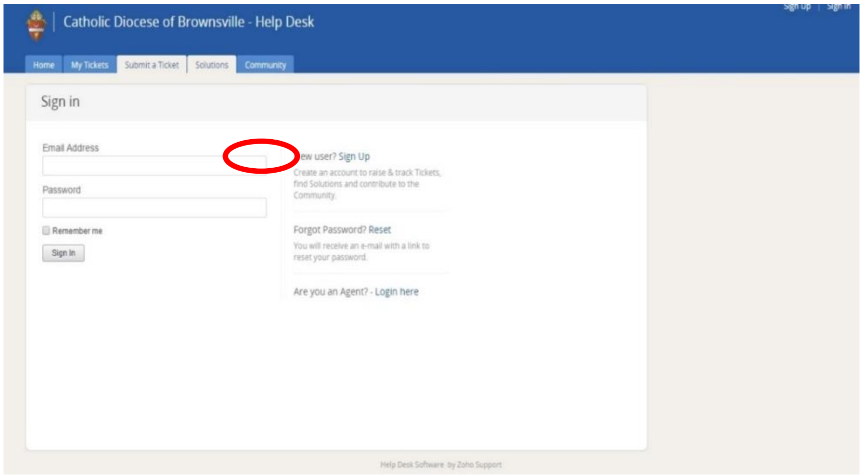
Any Help Desk request submitted at our Help Desk System is received by all CDOB I.T. Staff and responded according to our Service Level Agreement listed on page 9 of this document.

4.2 How to use the CDOB Help Desk System

To access the Diocese of Brownsville Help Desk website, type the following web address in your browser: https://helpdesk.cdob.org

There is also a blue button in the main page of our Diocesan Website

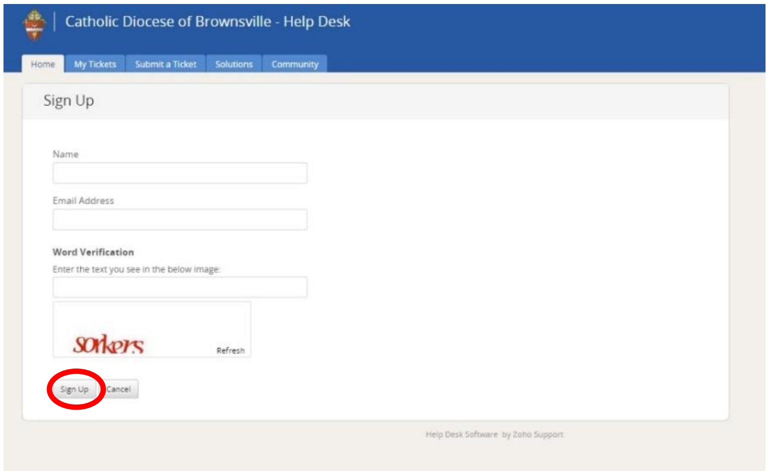
The following webpage will be displayed. To setup your Help Desk account, click the “Sign Up” link.



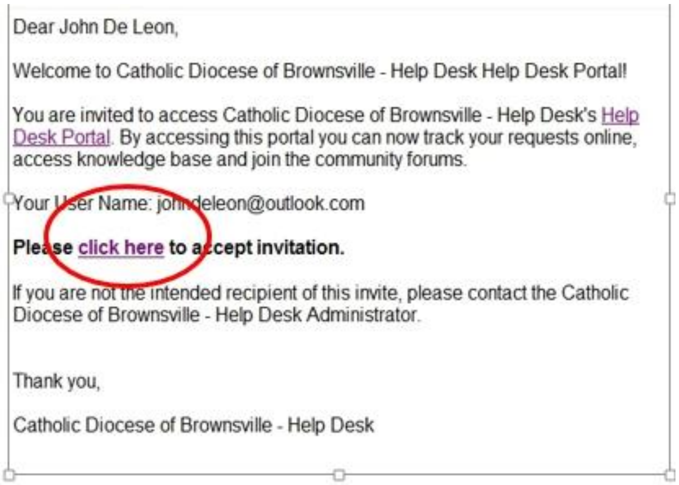
Create an account to raise & track Tickets, find Solutions and contribute to the Community.

You will receive an e-mail with a link to reset your password.

After selecting the “Sign Up” link above, the following webpage will display. Please enter your name, work email address for a Parish, School or Diocesan entity, Word Verification then click the Sign Up button. You can request a CDOB email account free of charge.


Catholic Diocese of Brownsville - Help Desk
Home
My Tickets
Submit a Ticket
Solutions
Community
Sign Up
Name
Email Address
Word Verification
Enter the text you see in the below image:
sorkers
Refresh
Sign Up
Cancel
Help Desk Software by Zoho Support

After clicking the “Sign Up” button above, you will receive an email from the Catholic Diocese of Brownsville – Help Desk, and will look similar to this image. Click, the “click here” link to accept the invitation.



Dear John De Leon,

Welcome to Catholic Diocese of Brownsville - Help Desk Help Desk Portal!

You are invited to access Catholic Diocese of Brownsville - Help Desk's Help Desk Portal. By accessing this portal you can now track your requests online, access knowledge base and join the community forums.

Your User Name: johndeleon@outlook.com

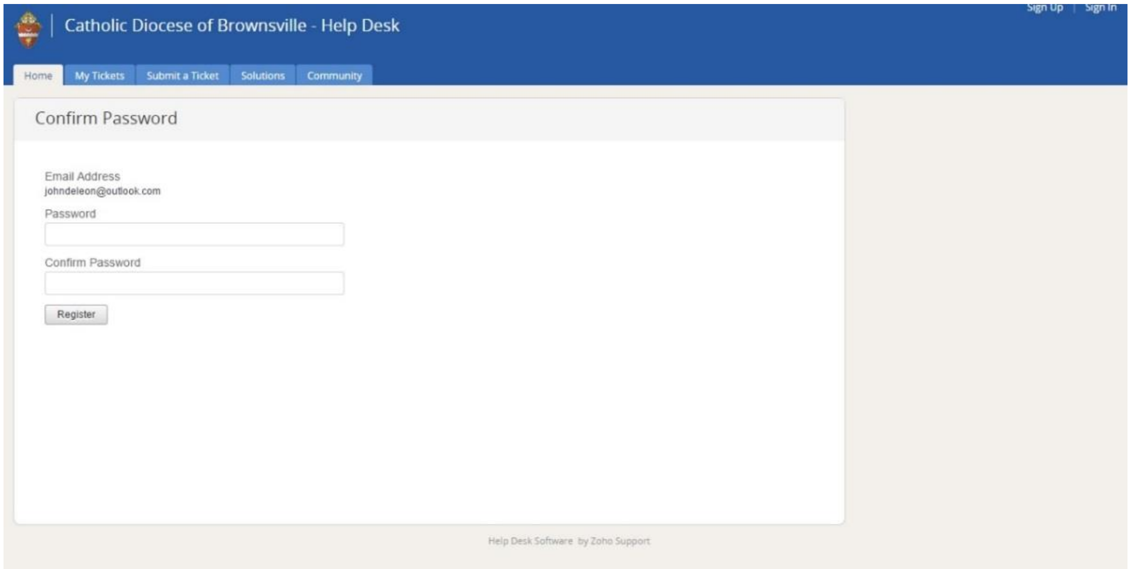
Please click here to accept invitation.

If you are not the intended recipient of this invite, please contact the Catholic Diocese of Brownsville - Help Desk Administrator.

Thank you,

Catholic Diocese of Brownsville - Help Desk

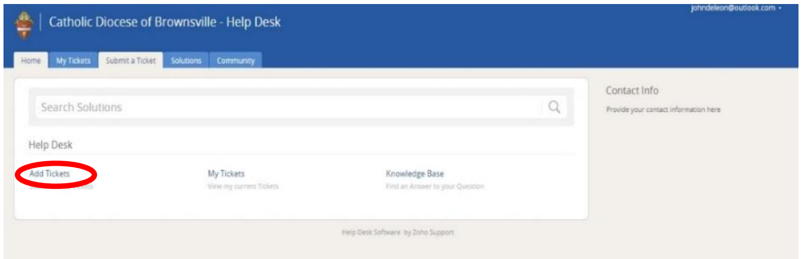
After clicking the “Click Here” link above, you will see the following webpage. Please follow the instructions to establish your password. It’s a good idea to use the same password that you’re currently using for your work email address (Parish, School or Diocesan entity).



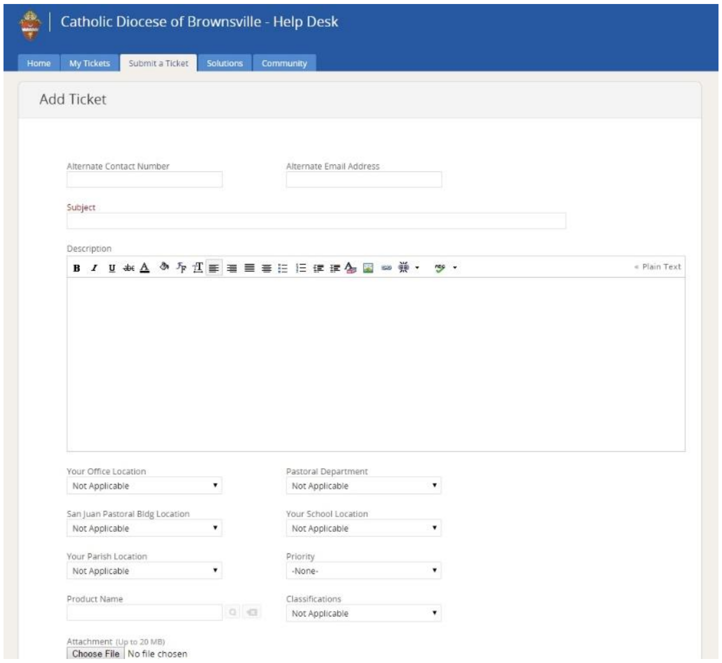
Confirm Password

Email Address
johndeleon@outlook.com

After you've established your password, you will see the following webpage. On the bottom row, you will see the following options; Add Tickets, My Tickets and Knowledge Base.



To create a Help Desk ticket, click the Add Tickets link on the bottom. The following webpage will display.



Add Ticket

Alternate Contact Number

Alternate Email Address

Subject

Description

Your Office Location: Not Applicable

Pastoral Department: Not Applicable

San Juan Pastoral Bldg Location: Not Applicable

Your School Location: Not Applicable

Your Parish Location: Not Applicable

Priority: -None-

Product Name

Classifications: Not Applicable

Attachment (Up to 20 MB) No file chosen

Please complete as much information as possible, including alternate contact number and email address if you cannot be reached at your desk or through the email account you used when you initially registered. Please be as descriptive as possible when describing your issue so that we can expedite a resolution for you. The more information you provide, the quicker we can find the root cause of your issue. Please be sure to select the appropriate drop-down list of items at the bottom of the page. You do not need to complete the Priority, Product Name or Classification selection. When complete, click the Submit button. Please submit one ticket per issue. Please do not combine multiple issues on one Help Desk ticket. To view previously submitted Help Desk tickets, click the My Tickets link at the bottom of the page to view updates etc.

Please refer to page 9, section 2.1 of this document for Help Desk response times.

5 Hardware Acceptable Use Policy

5.1 Computer Hardware

Hardware consists of the physical parts of a computer or other technology equipment. It includes Desktop/Laptop computers, Mobile and printing devices as well as the equipment needed to connect those computers to the CDOB network and the Internet.

5.2 Supported Hardware

The Information Technology supports the following hardware owned or leased by the Diocese of Brownsville or Affiliates:

- Computer Devices like: Servers, Desktops, Laptops
- Network Equipment like: Routers, Switches, Firewalls, Wireless Access Points
- Office Equipment like: Copiers, Printers, Fax Machines, Scanners, Phone Systems, Time Clocks.
- Mobile Devices like: Tablets, Mobile Phones

The CDOB has standardized on Dell equipment. Employees are assigned either a desktop or laptop computer, depending on their need. Loaner laptops are available for temporary use and requests are honored on a first-come, first-served basis. To request a loaner laptop, please contact the Help Desk.

5.3 Personal Hardware

In order to maintain a secure and virus-free computing environment, the CDOB does not permit personal hardware to be connected to the local area network (LAN) without prior authorization from the IT Department.

In addition, the IT department supports only CDOB issued equipment. Personal equipment, including that which is used on-site, is the responsibility of each employee. If an employee’s responsibilities require the use of equipment other than that issued by the CDOB, they should contact their supervisor, who may discuss the need with the Director of Information Technology.

The Help Desk can direct employees to alternate resources for technical support on computers used at home or for personal purposes.

5.4 Safeguarding of Hardware

All computer equipment should be safeguarded from damage, which may be caused by any of the following;

- Exposure to extremely high temperature or direct sunlight

- Exposure to extremely low temperatures
- Direct spills of liquids on computer components
- Reckless use of the equipment

5.5 Computer System Components

Any computer system component (e.g. monitor, printer, mouse etc.) should not be exchanged with other systems without the approval of the I.T. Department. (Brownsville and San Juan Offices)

5.6 Outside Consultants

User may not attempt or authorize outside consultants to perform modifications or repairs of any computer equipment without the approval of the I.T. Department.

5.7 Removal of Hardware

Removal of any equipment from the premises without proper authorization from the I.T. Department is strictly prohibited.

5.8 Printers, Copiers & Fax Machines

Printers, Copiers and Fax Machines should be used for business purposes only. Only the necessary pages in the document are to be printed and double sided printing is recommended.

Whilst printing is necessary in certain circumstances, it should be limited and carried out in an efficient manner. Desktop printers cost more to maintain and operate per page than networked printers, therefore, the provision of printers must be based on business needs and careful management is required to ensure efficient and effective use. All staff should be encouraged to consider the need to print and should consider using or storing electronic copies where possible.

Additional printers i.e. other than the network printers will only be allocated to an individual or work group in exceptional circumstances, based on a business need substantiated and approved by the IT Director or Moderator of the Curia.

Black-and-White printing should be used in preference to color printing.

Confidential information should be printed to either Local Printers when available or Network printers (Toshiba eStudio) that support “private codes”

The CDOB has a large number of printers, copiers and fax machines available for employee use. Most of the copiers also function as network printers, allowing you to send print jobs. Please contact the Help Desk for assistance with paper jams or any other technical issue. Supplies for printers and fax machines are the responsibility of each department or the Office Manager.

In San Juan to use the Toshiba e6550 color copier/printer you must have an access code. Access codes are entered in one of two ways:

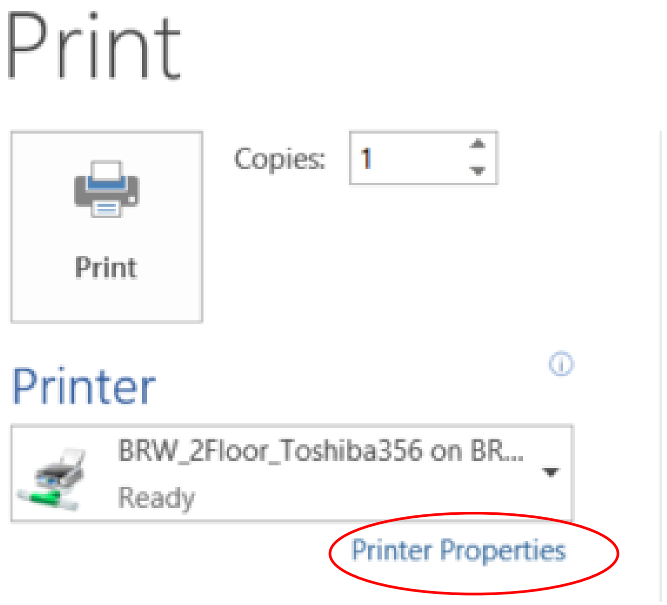
- While you are printing from your computer, you will see a pop-up box where you enter your copier access code.
- While at the copier.

The number of copies or print jobs made is tracked monthly and charges are allotted to the corresponding department.

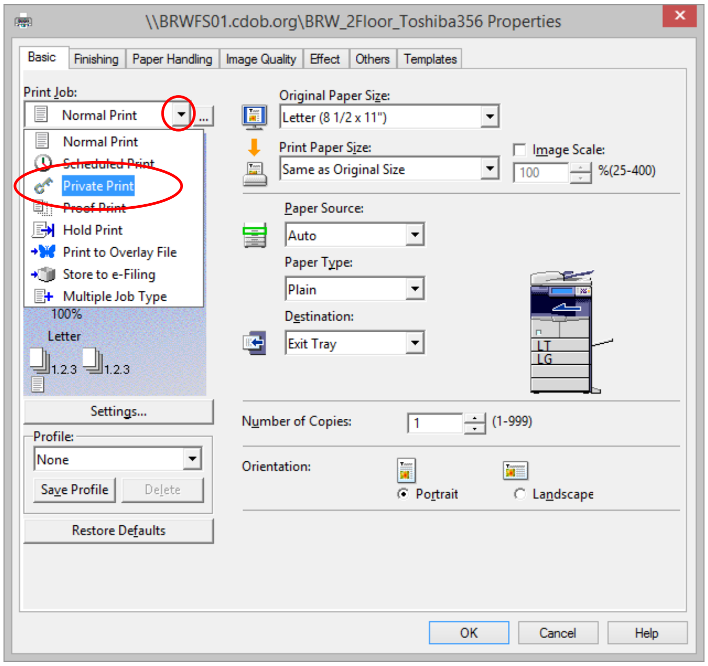
5.9 Printing Private Documents in Toshiba's eStudio Equipment

After selecting Print from your Windows Application (Word, Excel, Outlook, etc.)

1. Select "**Printer Properties**"



2. In “**Print Job Section**” click the “**Down Arrow**” and select “**Private Print**”



\\BRWFS01.cdob.org\BRW_2Floor_Toshiba356 Properties

Print Job: Normal Print

Original Paper Size: Letter (8 1/2 x 11")

Print Paper Size: Same as Original Size

Image Scale: 100 %(25-400)

Paper Source: Auto

Paper Type: Plain

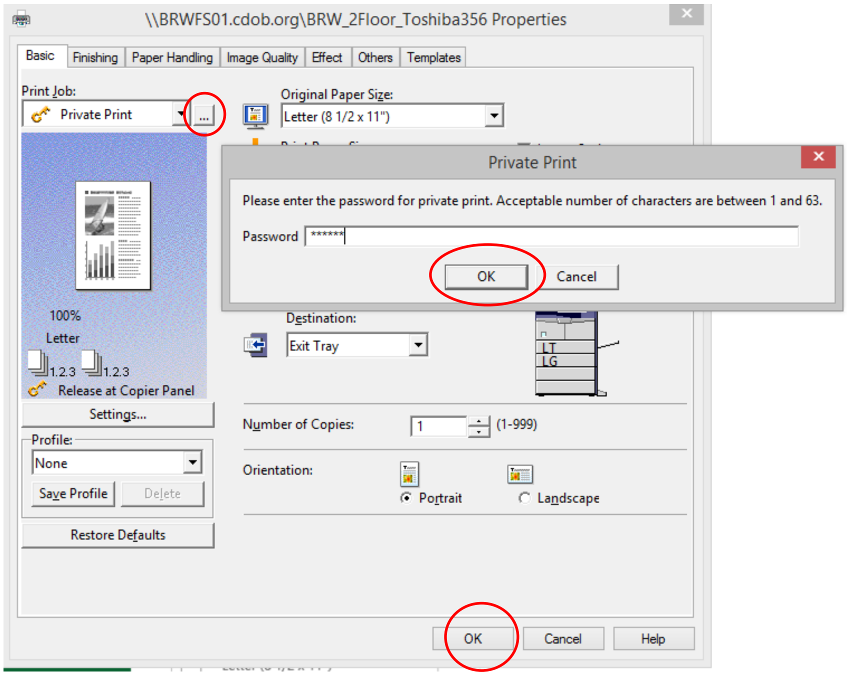
Destination: Exit Tray

Number of Copies: 1 (1-999)

Orientation: ● Portrait ○ Landscape

Profile: None

3. Click the **button with 3 points**, this will show up the “Private Print” Window; here type your **Private Print Code** and click “**Ok**” to close this Windows and click again **Ok** to exit the Printer’s Properties Window.



\\BRWFS01.cdob.org\BRW_2Floor_Toshiba356 Properties

Print Job: Private Print

Original Paper Size: Letter (8 1/2 x 11")

Private Print

Please enter the password for private print. Acceptable number of characters are between 1 and 63.

Password ******

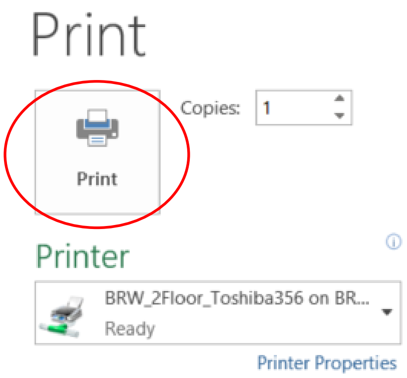
Destination: Exit Tray

Number of Copies: 1 (1-999)

Orientation: ● Portrait ○ Landscape

Profile: None

4. Now just click “Print”



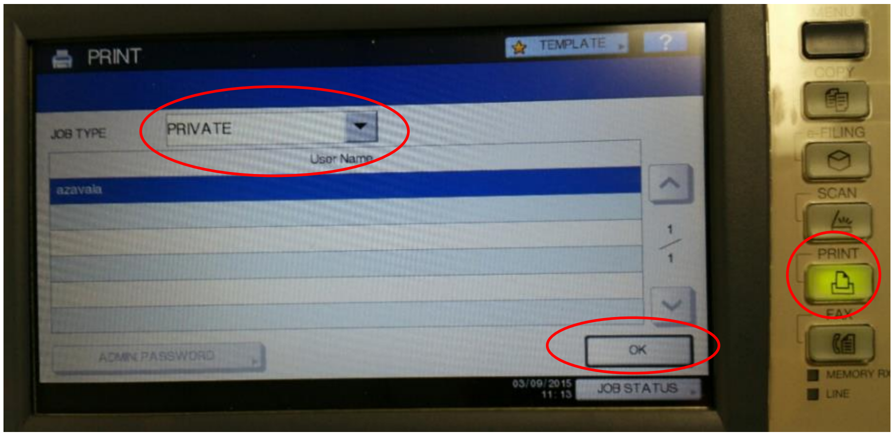
Print

Copies: 1

Printer

BRW_2Floor_Toshiba356 on BR...
Ready

5. At the printer; select the “**PRINT**” button, then select the Job Type: **PRIVATE** and click **OK**

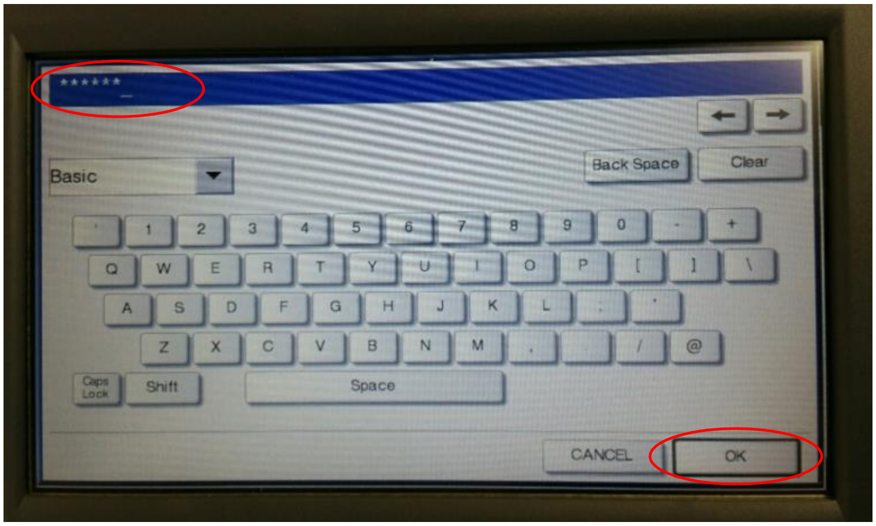


PRINT

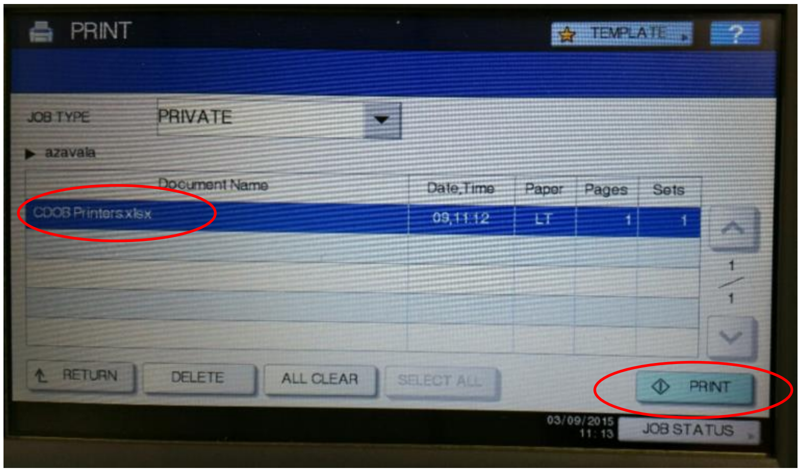
JOB TYPE PRIVATE

User Name
azavala

6. Now type your private code (from step 3) and press **OK**



7. **Select** your **Document** and then press “**Print**”



JOB TYPE PRIVATE

▶ azavala

Document Name	Date,Time	Paper	Pages	Sets
COOB Printers.xlsx	03,11:12	LT	1	1

1/1

03/09/2015 11:13

5.10 Installing a Network Printer

You can configure Windows to print to many different printers. Both local (connected directly to a PC) and network (shared through the local area network).

For assistance with printing, please contact the Help Desk.

6 Software Acceptable Use Policy

6.1 Personal Software

CDOB computer users are strongly discouraged from installing additional software (whether downloaded from the Internet or brought from home). Many applications can cause your computer to perform poorly or can have other adverse effects on your computer or the CDOB network. Some novelty programs with mass appeal (screen savers for example) may cause your computer to perform more slowly. Some programs have spyware or other malicious software secretly included. No software is truly “free”; there are hidden costs. All computers issued by the CDOB remain the property of the CDOB. Unauthorized software causing problems on a computer will be removed.

6.2 Acquisition of Software

All software acquired by the CDOB must be purchased by the I.T. department. Software acquisition is restricted to ensure that the I.T. department has a complete record of all software that has been purchased computers and can register, support and upgrade such software. The I.T. department will not provide support for software that has not been approved for purchase. All software installed on a computer system at any Diocesan office must have the appropriate licenses.

6.3 Software Installation

Software should be installed by the I.T. department. Manuals, tutorials and other user materials will be provided to the user (when available).

6.4 Software Responsibilities

All installed software must have a valid license and/or proof of purchase.

The I.T. department is responsible for software installed in its administrative offices, Affiliated Offices (such as Parishes, Schools, etc.) are 100% responsible for all software installed in their facilities, excluding Shelby.

6.5 Software Support

The I.T. department will support technical issues arising from software. We do not provide formal training on its usage. See section 18 “IT Resources” for online training options.

6.6 Software Audits

The I.T. department may conduct audits at any time on CDOB computers to ensure compliance with all software licenses.

6.7 Non-Business Files

Personal files (e.g. research papers, resumes, school work, reports, music etc.) are not allowed.

6.8 Games

No software games are allowed.

6.9 Peer-to-Peer Sharing

No peer-to-peer sharing of files is allowed.

6.10 Transfer of Files

Transfer of information to and from not-owned CDOB computers is not allowed.

6.11 Software Removal

Removal of any software without proper I.T. department approval is strictly prohibited.

6.12 Copyright Material

- CDOB believes in respecting and protecting the rights of intellectual property. This is not only a question of ethics, but also the law.
- CDOB reserves the right to monitor end user systems and the content stored therein. CDOB also reserves the right to remove, delete, modify or otherwise disable access to any materials found to be infringing on copyright.
- By reading and signing a copy of this policy, an employee of CDOB will not hold the CDOB responsible for any breach of a copyright law.
- No employee of CDOB may reproduce any copyrighted work in violation of the law. Works are protected by US copyright law even if they were not produced in the US.
- Copyrighted materials in the US are not required by law to be registered, unlike patents and trademarks, and may not be required to carry a copyright symbol. Therefore, copyrighted material may not be immediately recognizable. Assume material is copyrighted until proven otherwise.
- If a work is copyrighted, you must seek out and receive express written permission of the copyright holder to reproduce the copyrighted work in order to avoid violation.
- Copyrighted works include, but are not limited to: Text (e.g. articles), images (e.g. photographs), graphics (e.g. logos), sound recordings (e.g. MP3's), video recordings (e.g. movies) or software programs.

7 Office 365 & LAN Usage Policy

The CDOB has established a policy with regard to access and disclosure of any electronic files (email and text messages, documents, pictures, video and audio files, etc.) created, sent or received by Diocesan employees using either the CDOB Office 365 System and/or the CDOB LAN. These two systems will be referred as “CDOB IT System”

7.1 CDOB Office 365 System

CDOB manages a Microsoft Office 365 System, which includes: Email System (Exchange / Outlook), Lync, Yammer, OneDrive and SharePoint. This system is provided by the CDOB to assist in conducting business with the Diocese.

7.2 CDOB LAN

CDOB Manage a Local Area Network (LAN) which includes: Networking Equipment, Servers, Storage Devices, Desktop Computers, Laptop Computers, Mobile Devices, Printers and other devices. This LAN is provided by the CDOB to assist in conducting business with the Diocese.

7.3 Proprietorship

All content (email and text messages, documents, pictures, video and audio files, etc.), composed, sent or received by any CDOB IT System are and remain the property of the CDOB. They are not the private property of the employee, and employees may not consider any email messages or material as private or as their personal possession.

7.4 Personal Business

The use of any CDOB IT System is reserved solely for the conduct of business at the CDOB. Personal business should not interfere with the day-to-day operations of the CDOB.

7.5 Solicitations

Any CDOB IT System may not be used to solicit for commercial ventures, political causes, outside organizations or other non-job related solicitations.

7.6 Offensive Messages/Content

Any CDOB IT System is not to be used to create any offensive or disruptive messages/content. Among those which are considered offensive are any messages/content which contain sexual implications, racial slurs, gender specific comments or any other comment that offensively addresses someone’s age, sexual orientation, religious or political beliefs, national origin, ancestry or disability. In addition, any CDOB IT System must not be used to communicate other improper messages (e.g. messages or material that is defamatory, derogatory, obscene or otherwise inappropriate). The

CDOB IT System should not be used to commit any crime, including but not limited to sending obscene emails/txt messages or files with the intent to annoy, abuse, threaten or harass another person.

7.7 Chain Letters

Employees must not execute, send or forward chain letter emails.

7.8 Viruses

Employees may not use the CDOB IT System to develop or send any virus or otherwise destructive program. Employees should not open emails or attachments if unsure of the identity of the sender. Employees should use extreme caution when opening emails with attachments even when knowing the identity of the sender. If something looks strange in any part of an email, please contact the Help Desk.

7.9 Copyrighted Material

The CDOB IT System may not be used to send or receive copyrighted materials, trade secrets, proprietary financial information or similar materials without proper authorization.

7.10 Auditing

CDOB reserves and intends to exercise the right to review, audit, intercept, access and disclose all content created, received, sent or stored in any CDOB IT System for any purpose. Any content properly obtained for legitimate business purposes may be disclosed without the permission of the employee.

7.11 Confidentiality

The confidentiality of any message or file should not be assumed. Even when messages/files are deleted, it is still possible to retrieve and read them. Therefore, the use of passwords for security does not guarantee confidentiality.

7.12 Retrieval of Emails

CDOB has the right to retrieve and read any email messages.

Email messages must be treated as confidential by the employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any email messages that are not sent directly to them. Any exception to this policy must receive prior approval by the I.T. Department. This does not apply to emails where an employee has been designated as a “Delegate” for another employee’s email etc.

8 Social Media Acceptable Use Policy

8.1 Policy Coverage

With the continuing evolution of new media and next generation communications tools, the way in which the Diocese, parishes, schools, employees, and students can communicate internally and externally continues to develop at a rapid pace. While this creates new opportunities for communication and collaboration, it also creates new responsibilities. This policy has been developed to define the responsibilities of parishes, schools, and other affiliates in the use of these communication tools.

8.2 Authorization

A parish, school, or affiliate (such as cemeteries) may have a social media presence only with the expressed, written consent of the pastor, principal, or affiliate director.

8.3 Accountability

Each site must have at least two site administrators, a primary and a back-up, who can monitor and, if necessary, respond timely to communication on the site. All administrators must be adults who have been screened and had a background check. (Similar to the expectations of our parent chaperones). Passwords and names of sites should be registered in a central location, and more than one adult should have access to this information (i.e., site administrators and the pastor and/or principal).

8.4 Official Sponsorship

Electronic communications coming from a parish, school, or affiliate must be made through officially-sponsored technology meaning the entity being represented has to own the site, service, or account. In furtherance of this policy:

1. Every parish, school, or affiliate, to the extent that it has a website, must have its own appropriate domain (website address, also known as a URL).

    - Example: www.hsparish.org for Holy Spirit Parish McAllen

2. Any electronic communication coming from a parish, school, or affiliate must be on a domain for the corresponding parish, school, or affiliate.

    - Example: Secretary@hsparish.org, Info@hsparish.org.
    - Priests are encouraged to use an email from either the Diocese (cdob.org) or one with the parish name incorporated.

- It is expected that parish staff eliminate the use of free domains such as AOL, Gmail, Hotmail, Yahoo and other such services when representing the parish via email correspondence. Adherence to this recommendation will establish an authenticity of the correspondence and reduce the potential for misrepresentation/impersonation.

3. Personal sites, email addresses, etc., must never be employed as a substitute. For example, a Facebook announcement regarding an event for parish youth must be through a Facebook page for the parish, not a youth minister's personal Facebook page.

4. All clergy and personnel are encouraged to archive email and calendar activities affiliated with church business or pastoral care.

5. The Diocese of Brownsville maintains a record of all unit domains and email addresses of primary staff/volunteers and passwords. This information should be provided annually during the directory update process conducted by the diocesan director of communications. The Diocese of Brownsville reserves the right to modify postings as it deems necessary.

6. Every effort should be made to channel Facebook pages (ministries) through a central administrator – The Diocesan IT Director.

7. Official web pages must incorporate a brief but immediately apparent Code of Conduct for visitors to the page. Anyone who does not abide by the Code of Conduct should be blocked by the page administrator.

8.5 Adult Electronic Interaction with Minors

Electronic communication with minors must not be undertaken lightly. School, parish, and organization employees and volunteers must consistently adhere to Catholic values and transparency with respect to such communications.

1. All communication with minors (in person, via social media, websites, text messages, etc.) must adhere to:

    - The Charter for the Protection of Children and Young People (http://usccb.org/issues-and-action/child-and-youth-protection/charter.cfm)

    - The Children's Online Privacy Protection Act (http://www.ftc.gov/ogc/coppa1.htm)

2. Adults must not be in electronic communication with youth (under 18) unless the parents/guardians have authorized the communication. The authorization must identify the type of communication (e.g., email), the youth's specific contact information (e.g., email address), and contact information for the parents/guardians to ensure they receive copies of such communications. Parents must have access to everything provided to their children and be made aware of how social media is being used, be told how to access the sites, and be given the opportunity to be copied on all material sent to their children via social networking (including text messages).

3. Electronic copies of communications with minors must be preserved.

4. Schools receiving federal funding for computer technology through E-Rate must comply with the Children's Internet Protection Act (CIPA), 47 U.S.C. § 254(h)(5), which requires monitoring internet use by minors; filters to restrict access to obscenity, child pornography, or other material harmful to minors; and educating minors about appropriate online behavior, social networking safety, and cyberbullying.

8.6 Transparency, Honesty and Discretion in the Use of Social Media on Behalf of Parishes, Schools and Organization's.

Employees and volunteers are responsible for the information they divulge through social media. Employees and volunteers are subject to the following rules when posting information in connection with a parish, school, or organization:

1. Be honest about the facts and your identity.

2. Do not claim to represent the official position of the organization or the teachings of the Church unless authorized to do so.

3. Do not disclose confidential or proprietary information. Think carefully about whether the information being disclosed is ready for public consumption.

4. Do not disclose information protected from disclosure by law, such as medical information about employees or their identifying information (e.g., social security number).

5. Do not use diocesan, school, parish, or organizational trademarks or logos unless you are specifically authorized to do so.

6. Use good taste and discretion in all communication, including the content of photos and videos. Ensure that all content and links comply

with the Children's Internet Protection Act which, among other things, prohibits content that is obscene, pornographic, or otherwise harmful to minors.

7. Never cite others, or post text, photos, or videos of another person without permission.
    - Abide by civil law, including intellectual property protections, copyright and fair use laws, and IRS financial disclosure regulations.

8. Include a disclaimer stating that the views expressed are your own and not those of the diocese, or your parish, school, or organization, when commenting on an issue if you do not have specific authorization to speak on behalf of the Diocese, or your parish, school, or organization.

9. Do not violate the terms of agreement of the social media platform you are using.

10. Do not post pictures or video without first obtaining a signed Media Relations/Promotion Form for each individual shown.
    - Do not post pictures, video, or any other information that may identify a minor (e.g., name or contact information) without first obtaining permission from the parent or guardian and a signed Media Relations/Promotion Form.
11. Obtain parental/guardian permission for in-classroom social media activities.

8.7 Adhering to the Church's Doctrines and Teachings and to Diocesan/Parish Policies and Guidelines.

The content of electronic communication must not be at variance with the doctrinal and moral teaching of the Church. All communication by means of social media by parish/school/organization personnel is a reflection on the employee's parish/school/ organization, as well as on the entire Diocese. As a result, this communication must be representative of the policies and practices of the Diocese of Brownsville. The following rules have been adopted to support the foregoing policy:

1. Write in thoughtful language consistent with the message of Diocese of Brownsville and the Catholic faith.

2. Do not utter insults, slurs, or obscenities. Do not post anything that might be viewed as pornographic, proprietary, harassing, abusive, or creating a hostile work environment.
3. Do not disparage other individuals, other community groups, or other faiths.

4. Understand that electronic communications and social media activities are subject to other personnel policies, including non-discrimination/non-harassment and electronic communications policies.

5. Report social media activities that potentially violate this policy.

8.8 Personal Use of Social Media

Personal sites of church and school personnel should reflect Catholic values. Church and school personnel must understand that they are witnessing to the faith through all of their social networking, whether “public” or “private.” In furtherance of this policy, the Diocese has adopted the following rules:

1. "Friending" youth on social networks can be misinterpreted. Diocesan policy is to prohibit teachers, priests, and other employees from using their personal blogs, web pages, Facebook accounts, or e-mail to communicate with students or other parish youth. Such communications, if any, must be through officially sponsored social media pages to which the Diocese has access.

2. Employees and volunteers must exercise care with respect to privacy settings, personal profile information, and posted content to ensure that their use of social media and the internet does not reflect poorly on the churches, schools, or organizations for whom they work or conflict with Catholic beliefs and values.

3. Employees and volunteers must not identify themselves as employees or volunteers of the diocese or of any particular parish, school, or organization within the diocese on their personal social media pages unless they include a clear disclaimer stating, "The views expressed on this site are mine alone and do not necessarily reflect the views of my employer."

4. Employees are not permitted to use the logos, trademarks, official photographs, or any other intellectual property of the Diocese of Brownsville or its parishes (churches), schools, organizations, or programs in their personal blogs, web pages, or social media activities.

9 Network Security Policy

The security of the CDOB network is the responsibility of each employee. The following practices help keep our network secure.

9.1 Lock Your Computer When Away

Your computer is a powerful tool intended to help you perform your job more effectively. However, when left unprotected, it can be used inappropriately jeopardizing your files, other users' files, communications and the network itself.

All CDOB network computers have a 20 minute timer of inactivity at which point the computer or laptop will lock itself.

To manually lock/unlock your computer, press the CTRL+ALT+DEL buttons and follow screen instructions.

9.2 Passwords

All computers connected to the CDOB network require a password. When choosing a password, select one that is easy to remember, but hard for someone else to guess. Avoid using names of your family members, pet names and the car you drive. Your CDOB password should not be the same as the password used for any other purpose.

You should never share your network password with anyone else. If you need to share your files with someone in your department, or if you need to give another employee access to your email or calendar, contact the Help Desk for assistance.

Office 365 and Website passwords should be configured with Multi-Factor Authentication.

Please do not keep a written record of your password near your computer.

9.3 Password Requirements

The system automatically checks the password you enter. The password must meet the following minimum requirements;

- Must be changed every 90 days.
- Cannot be re-used for a time period.
- Must be at least 6 characters in length.
- Must contain both letters and numbers.

9.4 Failed Login Attempts

Users are allowed 3 attempts to login to the CDOB network. After 3 unsuccessful login attempts, your account is locked for 15 minutes. You can wait 15 minutes and try to log on again or call the Help Desk and have your password reset.

10 Computer Use and Internet Policy

The Internet is an important resource for the CDOB to provide better, cheaper and faster services to parishes and schools. The CDOB will creatively use the Internet to improve services and contribute broadly to the mission of the Church. The connection to the Internet and related facilities provided by the CDOB (the "Internet facilities") exist to facilitate the official work of the CDOB.

The Internet facilities are provided for employees and authorized persons affiliated with the CDOB for the efficient exchange of information and the completion of assigned responsibilities consistent with the mission of the CDOB.

The use of the Internet Facilities by any employee or other person authorized by the CDOB (the "Users") must be consistent with this Policy (including all security and confidentiality provisions set forth therein).

10.1 Principles of Acceptable Use

CDOB Internet Users are required:

- To respect the privacy of other Users; for example, Users shall not intentionally seek Information on, obtain copies of, or modify files or data maintained by other Users, unless explicit permission to do so has been obtained.
- To respect copyright and license agreements for software, digital artwork, and other forms of electronic data.
- To protect data from unauthorized use or disclosure as required by state and federal laws and CDOB regulations.
- To respect the integrity of computing systems: for example, Users shall not use or develop programs that harass other Users or infiltrate a computer or computing system and/or damage or alter the software components of a computer or computing system.
- To limit personal use of the Internet Facilities and equipment to that which is incidental to the User's official assignments and job responsibilities.
- To safeguard their accounts and passwords. Accounts and passwords are normally assigned to single Users and are not to be shared with any other person without authorization. Users are expected to report any observations of attempted security violations.

10.2 Unacceptable Use

It is not acceptable to use CDOB Internet facilities for activities unrelated to the mission of the CDOB, including:

- For activities unrelated to official assignments and/or job responsibilities, except incidental personal use in compliance with this Policy.
- For any illegal purpose.
- To transmit, receive, or access threatening, libelous, defamatory, sexual, obscene or harassing materials or correspondence.
- For unauthorized distribution of CDOB data and information.
- To interfere with or disrupt network Users, services or equipment.
- For private purposes, whether for-profit or non-profit, such as marketing or business transactions unrelated to CDOB duties.
- For any activity related to political causes.
- To advocate religious beliefs or practices contrary to Roman Catholic teaching.
- For private advertising of products or services.
- For any activity meant to foster personal gain.
- Revealing or publicizing proprietary or confidential information.
- Representing opinions as those of the CDOB.
- Uploading or downloading commercial software in violation of its copyright.
- Downloading any software or electronic files without reasonable virus protection measures in place.
- Intentionally interfering with the normal operation of any CDOB Internet traffic.

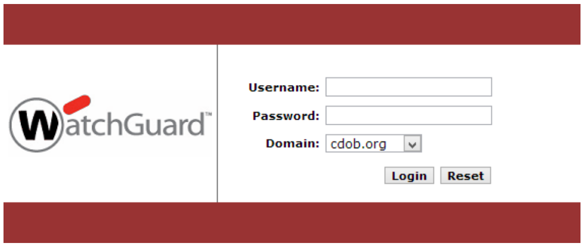
10.3 Internet Access Authentication

The CDOB utilizes a Firewall (WatchGuard) to protect our network from viruses, malware and inappropriate websites.

In order to browse the Internet, you must first be authenticated by WatchGuard. In order to get authenticated you should Login to the CDOB Network or use the WatchGuard authentication webpage: https://10.0.1.4:4100

When using the Authentication webpage, the following screen will display. Please type your CDOB computer log in name and CDOB computer log on password. Please ensure that the "Domain" selected is "cdob.org", if not click the drop-down arrow and select it.

Online time should be used for official purposes only.



Domain: cdob.org

10.4 Monitoring and Filtering

The I.T. department may monitor any Internet activity occurring on CDOB equipment or accounts. The I.T. department currently does employ WatchGuard filtering software to limit access to sites on the Internet. If the I.T. department discovers activities which do not comply with applicable law or department policy, records retrieved may be used to document the wrongful content in accordance with due process.

10.5 Downloading Files

When downloading documents from the Internet, the CDOB requires that such documents be job related and constitute a reasonable use of the CDOB resources. Programs files may not be downloaded without prior authorization. Files and programs downloaded may contain viruses. Users' must ensure that files are certified not to have viruses or that the files being received are from a reliable source. If it is not known who sent the email, attached files should not be downloaded.

10.6 Antivirus

The I.T. department utilizes Trend Micro Antivirus on all computers and laptops that connect to the CDOB Network. Trend Micro Antivirus is continually updated with the latest virus definition files in order to detect virus threats. While Trend Micro uses the latest definition files to catch viruses, there's no guarantee that all threats will be detected.

10.7 Sexually Explicit Sites

The CDOB Internet must not be used to visit sexually explicit or otherwise offensive or inappropriate web sites or to send, display download or print offensive material, pornographic or sexually explicit pictures or any other materials.

10.8 Internet Disclaimer

CDOB assumes no liability for any direct or indirect damages arising from the users' connection to the Internet. CDOB is not responsible for the accuracy of information found on the Internet and only facilitates the accessing and dissemination of information through its systems. Users are solely responsible for any material that they access.

11 Sensitive Data Protection Policy

11.1 Purpose

To protect Catholic Diocese of Brownsville sensitive data from unauthorized disclosure and inappropriate use.

11.2 Scope

This policy applies to all Catholic Diocese of Brownville employees.

11.3 Policy

It is the responsibility of everyone with access to sensitive data resources to use these resources in an appropriate manner and to comply with all applicable federal, state, and local statutes. Additionally, it is the responsibility of everyone with access to sensitive data resources to safeguard these resources. Methods of safeguarding sensitive data include:

- Do not store sensitive data on office desktop computers.

- Do not store sensitive data on mobile devices, such as, laptops, notebooks, tablets, USB devices, CDs, DVDs, mobile phones, etc., that are easily stolen or compromised.

- Do not store sensitive data on Office 365 System (Outlook Email, OneDrive for Business, SharePoint, etc.) or any other Cloud Storage System.

- Access to sensitive data resources in either electronic or physical form should be restricted only to those individuals with an official need to access the data.

- All Servers and File Cabinets containing sensitive data must be housed in a secure location and operated only by authorized personnel.

- Lock your computer (CTRL+ALT+DELETE) anytime you leave your desk.

- Practice a clean desk policy by securing all sensitive data contained in documents, CDs, DVDs, USB drives, etc., under lock and key when you leave your desk.

- Sensitive data should be only transmitted by email in a secure manner using data encryption transmitted via secure socket layer.

- Sensitive data must be encrypted anytime it has to be uploaded to another site. The website MUST use HTTPS or SSL encryption. If you are required to use FTP or Telnet, you must use the encrypted versions of these protocols, e.g., SSH and SFTP. There are no exceptions. If you need assistance, contact the Help Desk at helpdesk@cdob.org or call (956) 550-1500.

- Any accidental disclosure or suspected misuse of sensitive data should be reported immediately to the IT Director and Human Resources Director.

- Dispose of sensitive data securely by shredding paper documents, and formatting or Destroying Hard Disks.

11.4 Applicability

All Catholic of Diocese employees. Applies to all individuals who have access to sensitive data, including but not limited to social security numbers, credit card numbers, bank accounts, computer passwords, date of birth, driver license number and any personal information flagged for non-disclosure.

11.5 Definitions

Sensitive Data - any information that is protected by Federal and Texas law. Examples of sensitive data include but are not limited to:

- Social Security Numbers (SSN)
- Credit card numbers and banking information.
- Personal Passwords.
- Protected Health Information (PHI).
- and any personal information flagged for non-disclosure.

PHI - under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity) and can be linked to a specific individual.

11.6 Enforcement

Violation or non-compliance of this policy may result in disciplinary action up to and including termination of employment.

12 Data Breach Response Policy

12.1 Purpose

The purpose of this policy is to establish the steps to follow for a data breach incident in the Catholic Diocese of Brownsville. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

Catholic Diocese of Brownsville Information Security is committed to protect Catholic Diocese of Brownsville's employees, partners and the organization from illegal or damaging actions by individuals, either knowingly or unknowingly.

12.2 Background

This policy mandates that any individual who suspects that a theft, breach or exposure of Catholic Diocese of Brownsville Sensitive data has occurred must immediately report it to the IT Director and Human Resources Director.

12.3 Scope

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle sensitive data (personally identifiable information or Protected Health Information) of Catholic Diocese of Brownsville employees.

12.4 Action Plan

- Take affected equipment offline.
- Reset affected user/system password(s).
- Scan affected computer for malware/viruses.
- Interview people who discovered the breach and document your investigation.
- Inform Bishops and Director’s Department from the affected computer/user account about the incident.
- Depending of the size of the data breach, Bishops will decide if local authorities should be informed.
- If Electronic Health information has been compromised, check this link: https://hhs.gov/hipaa/for-professionals/breach-notification for more details.
- Notify affected people that their personal information has been compromised.
- If Bank account information has been compromised —say, credit card or bank account numbers notify the Bank, so that they can monitor the accounts for fraudulent activity.
- If names and Social Security numbers have been stolen, contact the major credit bureaus for additional information or advice. If the compromise may

involve a large group of people, advise the credit bureaus if you are recommending that people request fraud alerts and credit freezes for their files.

  - Equifax: equifax.com or 1-800-525-6285
  - Experian: experian.com or 1-888-397-3742
  - TransUnion: transunion.com or 1-800-680-7289

- Check with the Diocesan Human Resources Department if a "Free Credit Monitoring Service" is available.
- Work with Catholic Diocese of Brownsville communications, legal and human resource departments to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.
- Instruct affected people to access the following Web page: https://www.IdentityTheft.gov/databreach from the FTC (Federal Trade Commission) for information on appropriate follow-up steps after a compromise, depending on the type of personal information that was exposed. it's important to advise people to place a least a free 90 days fraud alert on their credit reports.
- The IT Department will analyze the breach or exposure to determine the root cause and take the appropriate actions to try to stop this from happening again.

12.5 Enforcement

Any Catholic Diocese of Brownsville employee found in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

13 CDOB Rights

Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq), notice is hereby given that there are NO facilities provided by this system for sending or receiving private or confidential electronic communications. System administrators have access to all email and will monitor messages as necessary to assure efficient performance and appropriate use. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

CDOB reserves the right to log network use and monitor file server space utilization by Users and assumes no responsibility or liability for files deleted due to violation of file server space allotments.

CDOB reserves the right to remove a User account from the network.

The CDOB will not be responsible for any damages. This includes the loss of data resulting from delays, non-deliveries, or service interruptions caused by negligence, errors or omissions. Use of any information obtained is at the User's risk.

CDOB makes no warranties, either express or implied, with regard to software obtained from the Internet.

CDOB reserves the right to change its policies and rules at any time.

CDOB makes no warranties (express or implied) with respect to Internet service, and it specifically assumes no responsibilities for:

- The content of any advice or information received by a User through the Internet Facilities or any costs or charges incurred as a result of seeking or accepting such advice;

- Any costs, liabilities or damages caused by the way the User chooses to use the Internet Facilities;

- Any consequence of service interruptions or changes, even if these disruptions arise from circumstances under the control of the CDOB.

CDOB Internet Facilities are provided on an as is, as available basis.

13.1 Enforcement of Violations

This policy is intended to be illustrative of the range of acceptable and unacceptable uses of Internet Facilities and is not necessarily exhaustive. Questions about specific uses related to security issues not enumerated in this policy statement and reports of specific unacceptable uses should be directed to the CDOB IT Director.

CDOB will review alleged violations of the Internet Acceptable Use Policy on a case by-case basis. Violations of the policy will result in disciplinary actions as appropriate, up to and including dismissal.

14 Information Technology Standards

The I.T. Department standards policy lists all technologies supported by the CDOB and serves as a guideline for all technology purchasing and use decisions.

The primary goal of developing and implementing a standards policy are;

- To ease purchasing decisions by pre-evaluating and pre-approving technology solutions.
- To reduce training and support costs by narrowing the number of technologies and products used.
- To ensure integration and interoperability between technologies.
- To set parameters for future technology and development.

Component	Current Standard
Desktop OS	Windows 8.1 PRO & 10 Pro
Server OS	Windows Server 2008 - 2019
Servers	Dell PowerEdge Line
Desktop	Dell OptiPlex Line
Laptop	Dell Latitude Line, Microsoft Surface Pro
Tablets	Apple iPad, Samsung Galaxy Tab
Internet Browser	Internet Explorer 10, 11 Google Chrome Firefox
Anti-Virus	Trend Micro
Office Suite	MS Office 2010, 2013, 2016
Desktop Publishing	Adobe Software
Email System	Microsoft Office 365
All-in-One Printers	HP, Toshiba and Dell
WAPs	Meraki, EnGenius & Aruba
Internet Access	Cable
Network Firewall	WatchGuard XTM, Series M
Ethernet Switches	HP, CISCO

For more information or help to implement any of these products, please contact the Information Technology Department.

15 IT Purchasing Policy

15.1 Scope

This policy covers all information technology hardware and software purchased with Catholic Diocese of Brownsville (CDOB) funds. Specifically, the scope of this policy includes, but is not limited to, the following CDOB technology resources:

- Desktops, Laptops, Tablets, Printers, Scanners, Monitors, Projectors, TVs, Phones, etc.
- Software.
- Most electronic equipment, audio recording equipment, digital cameras etc.
- Any wireless device.
- Any peripheral that attaches to a computer or laptop.

All hardware and software purchased with CDOB funds and/or Grant Money are the property of CDOB. This also includes all items purchased using a personal credit card for which the employee is later reimbursed.

15.2 Purchase of Standard Technology

Standardization allows CDOB to efficiently select and manage technology, obtain better technology pricing, reduce maintenance costs and increase access to training and assistance. These standards are re-evaluated periodically based on common needs, vendor offerings, cost, reliability, supportability, quality, sustainability and timeliness of vendor response. When technology is adopted as a CDOB standard it is considered to be pre-approved for purchase by the IT Department.

15.3 Purchase of Non-Standard Technology

Purchase of non-standard technology components should be minimal, and justified through extenuating circumstances. This includes technology purchased through grants and other non-CDOB funds. CDOB will not reimburse or support the purchase of any technology related item, unless that purchase was made through and/or with the knowledge and approval of IT Department.

15.4 IT Purchases Procedure

All purchase requests for any Information Technology (I.T.) related component (hardware / software) must first be reviewed/approved by the I.T. Director. This is to ensure that item(s) being purchased are compatible with our infrastructure and the purchase is feasible.

All requests must be submitted to any member of the I.T. department by the requestor's Department Director approving the purchase and specifying the following items:

- Final User
- Quantities and Item(s) description
- Reason / Justification of Purchase
- Account No. or Grant No. to be charged

Only if the purchase includes devices like Tablets, Phones, Cameras, Computers, Printers, Scanners, Digital recorders or any other major device, the purchase must be approved also (in writing) by either the Moderator of the Curia or Bishop.

It is the responsibility of the requesting department's Director to ensure that funds are in place prior the order placement.

All approved requests for items will be processed by the I.T. department staff once we receive the required authorizations.

15.5 Emergency Purchasing

Purchases may be made outside of the scope of this policy and without approval of the I.T. or department manager; however, the purchasing employees will still be held accountable for the purchase decision under the following circumstances:

- In the event of an emergency where purchasing items through regular channels and waiting for delivery may take too long.
- In the event that an employee or department needs specialized software or some other component that is not on the Standard items list, but is required to perform work or complete a project.

15.6 Confidentiality

In the context or organizational purchasing activities, employees may come into contact with pricing information which, if divulged to vendors, could negatively affect pricing negotiations. The sharing of vendor pricing information with competing vendor may also pose a threat to the relationship with vendors and could result in a breach of contract. All pricing information employees may come across in a purchase process must be maintained in strict confidentiality. Items including vendor contracts, purchase orders, evaluation tools and any other documented information involving leasing, acquisition or contracting of IT hardware, software, technical or other services must be maintained securely and held in strict confidence.

15.7 Conflict of Interest

To ensure fairness in bidding, any existing relationship between the purchasing employee and vendors involved in a competitive bid or otherwise must be declared. Those individuals involved in vendor selection must divulge existing relationships to ensure fair bidding process by ensuring no rewards are received by CDOB employees in exchange for awarding company contracts to the aforementioned vendors.

15.8 Non-Compliance

The purchase policy exists to ensure that financial commitments made by CDOB to vendors are accounted for and follow Purchasing Policy guidelines. Employees should be aware that they may be held accountable for rogue purchasing or any other commitments to vendors which occur outside the boundaries of this policy.

16 CDOB Network

Computers at the Chancery Office in Brownsville, San Juan Pastoral Center and Catholic Charities Buildings in San Juan are connected by using a Network; allowing computers to share network printers, file servers and other resources like Internet Access or remote Management.

16.1 File Management

CDOB Employees are strongly encouraged to store files on network drives or Office 365 Document Libraries, as opposed to on a local hard disk drive (C:\ or Desktop). Use of Public Internet Cloud Storage Services Like Dropbox, Google Drive, Box, etc; are not allowed. Network files are secure and back-up copies are made nightly. Files stored on your computer may not be recoverable if the hard drive (local disk C:\) fails. Computer hard drives are prone to failure; the best practice to store files is on your network drives or Office 365 Document Libraries.

<u>Please do not store files on your local hard disk drive (C:\). Instead, use network drives or Office 365 Document Libraries.</u>

Each employee has access to the following network drives and Office 365 Document Libraries:

CDOB Network Drives	Description
H:\	This is your "My Documents" file saving location. This is where you save all your files. Only you can access this folder.
P:\	Not commonly used. This is where server based applications are stored. You may never have to access this folder directly.
S:\	Share Folder. In this folder you can share documents with others in the network or access other departments' folders if permission has been granted.

Office 365 Documents Libraries	Description
OneDrive for Business	This is a **persona**l library intended for storing and organizing **your** work documents.
SharePoint Documents Libraries	These are **group** libraries intended for storing and organizing "**team"** work documents.

16.2 Email Messages Safeguarding

16.2.1 Cleaning Mailboxes

Email messages can quickly multiply. Many CDOB employees receive 50 or more emails every day. Office 365 mailboxes are 50 GB each. Although the mailbox size is really big, the space is limited; so, it is a good practice to clean out your Outlook folders (especially Inbox, Sent Items and Deleted Items).

Many users file messages into different folders within their Inbox. This helps organize your messages, but it does not help free space on the email system.

You can help by deleting, saving and archiving email messages.

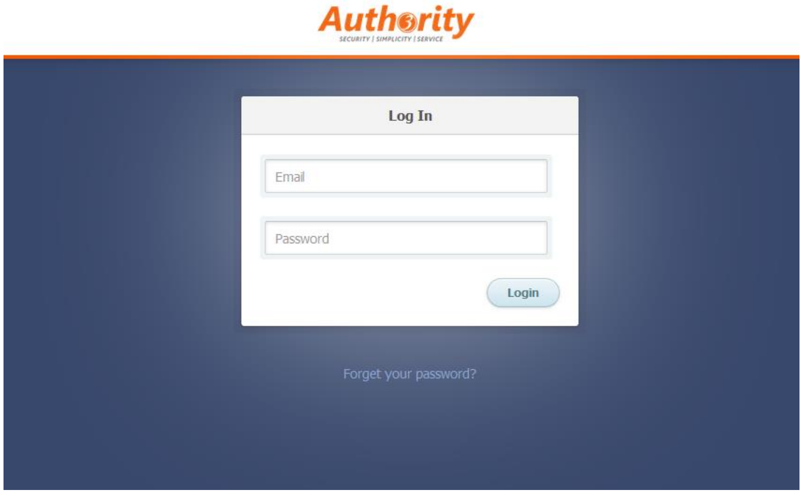
1. Delete junk, spam and all other messages you no longer need.
2. Move messages to your Archive Folder.

16.2.2 Email Accounts Backups and Archives

All deleted Email messages in Office 365, are retained for up to for 30 Days. User can recover deleted messages in Outlook by going to the "Deleted Items" folder; if the messages have been deleted from there, users can do a Right Click in "Deleted Items" folder and select "Recover Deleted Items". Also, in Outlook by Selecting the Tab "FOLDER" and then "Recover Deleted Items". Additionally, email accounts from Diocesan Directors, their Secretaries/Assistants and Key personnel are Backed Up on a daily basis and archived continuously by 3rd party services.

Users with Archive Service activated can access their Archive Account at:

https://apps.authority3.com/



Use your Email account as user ID and ask to the CDOB IT Help Desk for your password.

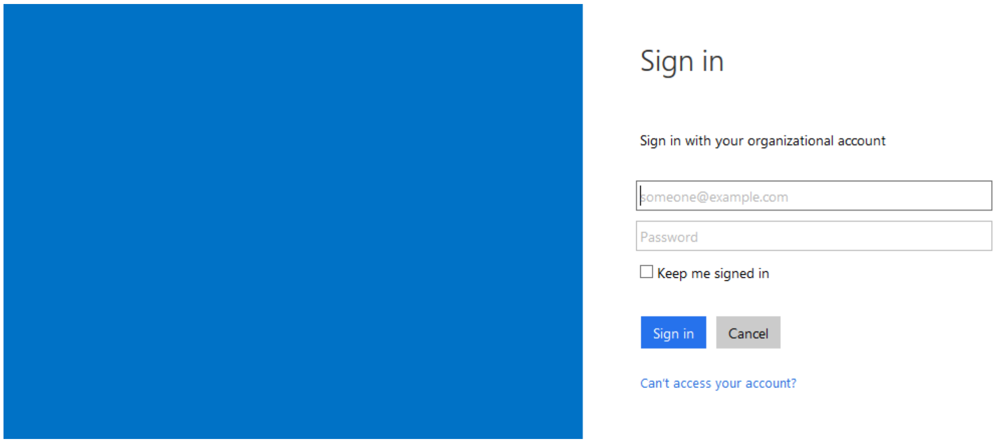
16.2.3 Email Filtering

All incoming email is scanned for viruses and spam. Any message with a suspected virus or spam is quarantined.

Our Email System send us “End-User Spam Notifications” every 7 Days; but if you need to check for an email sooner than that, you can access your own spam-quarantined messages via the web using the following link:

https://admin.protection.outlook.com/quarantine

(*Please add the above address to your Favorites List in your Browser)*



Sign in

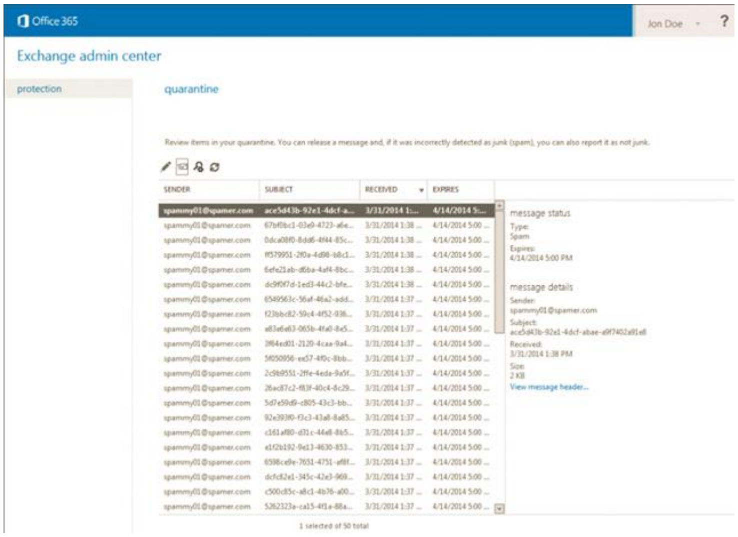
Sign in with your organizational account

someone@example.com

Password

□ Keep me signed in

Note: To *Sign in* use your **full email address** and **password**



Review items in your quarantine. You can release a message and, if it was incorrectly detected as junk (spam), you can also report it as not junk.

SENDER	SUBJECT	RECEIVED	EXPIRES
spammy01@spamer.com	ace5d43b-92e1-4dcf-a...	3/31/2014 1:...	4/14/2014 5:...
spammy01@spamer.com	67bf0bc1-03e9-4723-a6e...	3/31/2014 1:38 ...	4/14/2014 5:00 ...
spammy01@spamer.com	0dca08f0-8dd6-4f44-85c...	3/31/2014 1:38 ...	4/14/2014 5:00 ...
spammy01@spamer.com	ff579951-2f0a-4d98-b8c1...	3/31/2014 1:38 ...	4/14/2014 5:00 ...
spammy01@spamer.com	6efe21ab-d6ba-4af4-8bc...	3/31/2014 1:38 ...	4/14/2014 5:00 ...
spammy01@spamer.com	dc9f0f7d-1ed3-44c2-bfe...	3/31/2014 1:38 ...	4/14/2014 5:00 ...
spammy01@spamer.com	6549563c-56af-46a2-add...	3/31/2014 1:37 ...	4/14/2014 5:00 ...
spammy01@spamer.com	f23bbc82-59c4-4f52-938...	3/31/2014 1:37 ...	4/14/2014 5:00 ...
spammy01@spamer.com	e83e6e63-065b-4fa0-8e5...	3/31/2014 1:37 ...	4/14/2014 5:00 ...
spammy01@spamer.com	3f64ed01-2120-4caa-9a4...	3/31/2014 1:37 ...	4/14/2014 5:00 ...
spammy01@spamer.com	5f050956-ee57-4f0c-8bb...	3/31/2014 1:37 ...	4/14/2014 5:00 ...
spammy01@spamer.com	2c9b9551-2ffe-4eda-9a5f...	3/31/2014 1:37 ...	4/14/2014 5:00 ...
spammy01@spamer.com	26ad87c2-f83f-40c4-8c29...	3/31/2014 1:37 ...	4/14/2014 5:00 ...
spammy01@spamer.com	5d7e59d9-c805-43c3-bb...	3/31/2014 1:37 ...	4/14/2014 5:00 ...
spammy01@spamer.com	92e393f0-f3c3-43a8-8a85...	3/31/2014 1:37 ...	4/14/2014 5:00 ...
spammy01@spamer.com	c161af80-d31c-44e8-8b5...	3/31/2014 1:37 ...	4/14/2014 5:00 ...
spammy01@spamer.com	e1f2b192-9e13-4630-853...	3/31/2014 1:37 ...	4/14/2014 5:00 ...
spammy01@spamer.com	6598ce9e-7651-4751-af8f...	3/31/2014 1:37 ...	4/14/2014 5:00 ...
spammy01@spamer.com	dcfc82e1-345c-42e3-969...	3/31/2014 1:37 ...	4/14/2014 5:00 ...
spammy01@spamer.com	c500c85c-a8c1-4b76-a00...	3/31/2014 1:37 ...	4/14/2014 5:00 ...
spammy01@spamer.com	5262323a-ca15-4f1a-88a...	3/31/2014 1:37 ...	4/14/2014 5:00 ...

1 selected of 50 total

message status

Type:
Spam

Expires:
4/14/2014 5:00 PM

message details

Sender:
spammy01@spamer.com

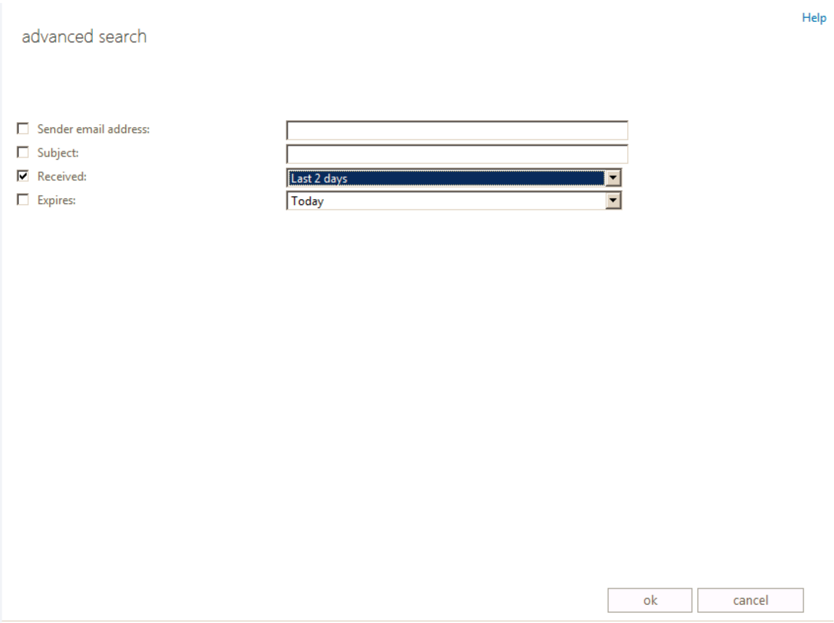
Subject:
ace5d43b-92e1-4dcf-abae-a9f7402a91e8

Received:
3/31/2014 1:38 PM

Size:
2 KB

View message header...

You can search your spam quarantine for a particular message, using criteria such as received date and subject in order to narrow down the list of messages shown.



advanced search

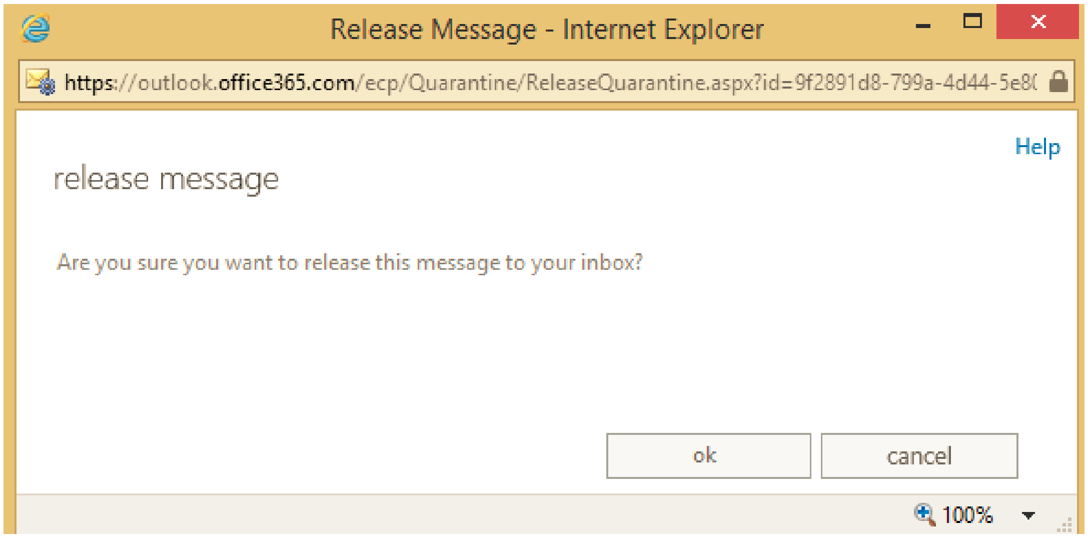
□ Sender email address:

□ Subject:

☑ Received: Last 2 days

□ Expires: Today

You can also release individual messages from your spam quarantine for delivery to your inbox.



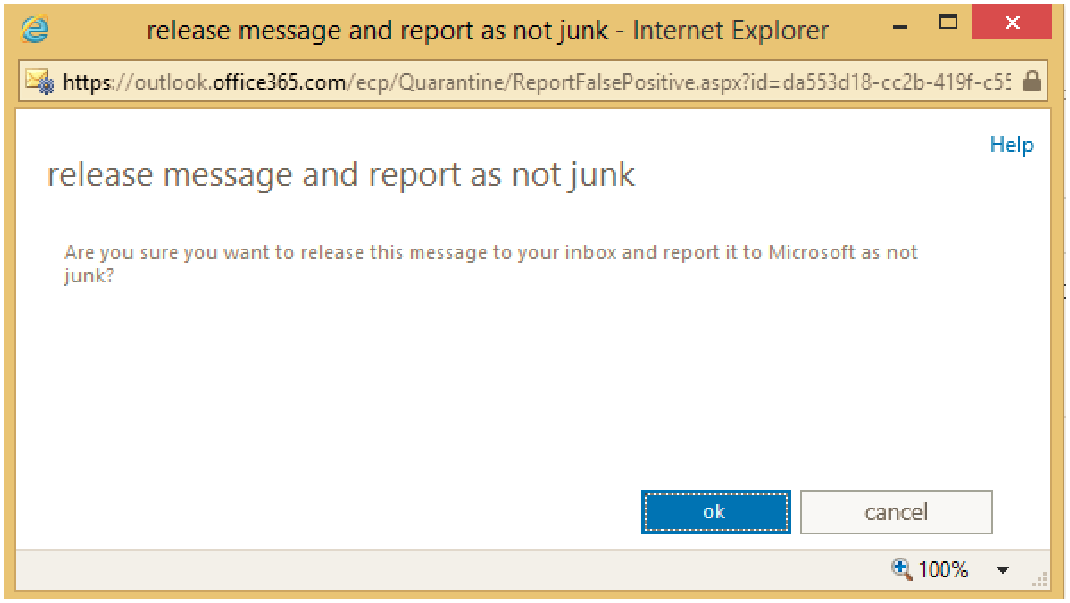
Release Message - Internet Explorer

https://outlook.office365.com/ecp/Quarantine/ReleaseQuarantine.aspx?id=9f2891d8-799a-4d44-5e8(

release message

Are you sure you want to release this message to your inbox?

In addition, you can report messages as “not junk” to the Microsoft Spam Analysis Team, who will evaluate and analyze the message. Depending on the results of the analysis, the service-wide spam content filter rules may be adjusted to allow the message through. Reporting the message as not junk also releases the message to your inbox.



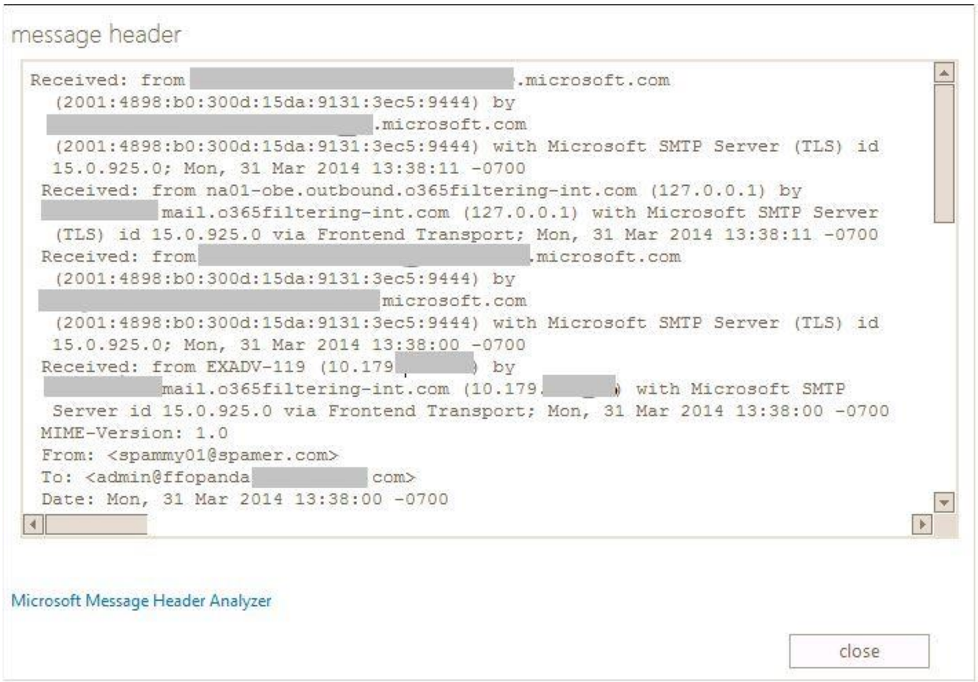
release message and report as not junk - Internet Explorer
https://outlook.office365.com/ecp/Quarantine/ReportFalsePositive.aspx?id=da553d18-cc2b-419f-c5
Help

release message and report as not junk

Are you sure you want to release this message to your inbox and report it to Microsoft as not junk?

When you report a message as “not junk,” it’s released to your inbox.

You can view details of how a message was received by clicking the View Message Header… link to get the SMTP header portion of the message. You can access the View Message Header… link on the page that lists all your spam-quarantined messages, under message details.



message header

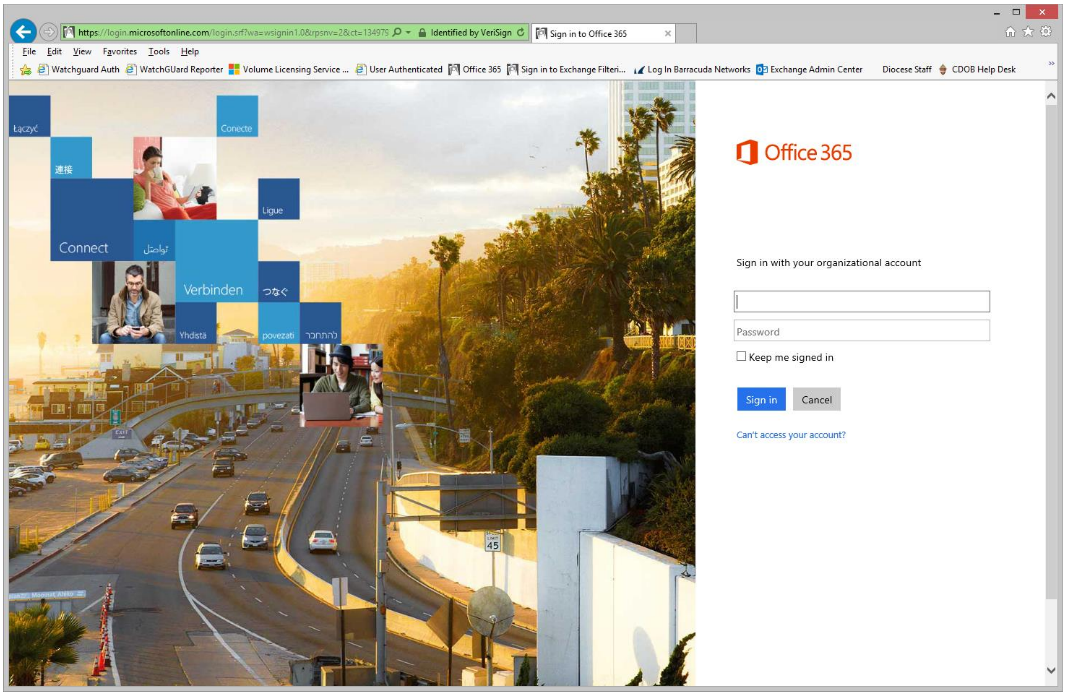
```
Received: from [redacted].microsoft.com
  (2001:4898:b0:300d:15da:9131:3ec5:9444) by
 [redacted].microsoft.com
  (2001:4898:b0:300d:15da:9131:3ec5:9444) with Microsoft SMTP Server (TLS) id
  15.0.925.0; Mon, 31 Mar 2014 13:38:11 -0700
 Received: from na01-obe.outbound.o365filtering-int.com (127.0.0.1) by
 [redacted]mail.o365filtering-int.com (127.0.0.1) with Microsoft SMTP Server
  (TLS) id 15.0.925.0 via Frontend Transport; Mon, 31 Mar 2014 13:38:11 -0700
 Received: from[redacted].microsoft.com
  (2001:4898:b0:300d:15da:9131:3ec5:9444) by
 [redacted]microsoft.com
  (2001:4898:b0:300d:15da:9131:3ec5:9444) with Microsoft SMTP Server (TLS) id
  15.0.925.0; Mon, 31 Mar 2014 13:38:00 -0700
 Received: from EXADV-119 (10.179[redacted]) by
 [redacted]mail.o365filtering-int.com (10.179.[redacted]) with Microsoft SMTP
  Server id 15.0.925.0 via Frontend Transport; Mon, 31 Mar 2014 13:38:00 -0700
 MIME-Version: 1.0
 From: <spammy01@spamer.com>
 To: <admin@ffopanda[redacted]com>
 Date: Mon, 31 Mar 2014 13:38:00 -0700
```

Viewing the message header for an individual message gives you details about how it was received.

16.3 Office 365 Web Access

You can access your Office 365 account, including your email from any computer with an Internet connection, at any of the following URL Addresses:

- outlook.cdob.org
- office.cdob.org
- login.microsoftonline.com
- www.cdob.org (Left Side, Middle page, there is an "envelop icon")



Sign in with your organizational account

Password

☐ Keep me signed in

Can't access your account?

Once you are connected you will be able to view your email, calendar, People (contacts) OneDrive, Yammer and SharePoint. Links for these services will be located in the upper right hand side of the screen. For online training options see section 18 "IT Resources"

16.4 Calendar

Microsoft Outlook is the standard calendar system in use by the CDOB. You can use the Outlook calendar to track your meetings and appointments (both professional and personal/private), and to schedule meetings with others.

The calendar is most effective when everyone uses it. When you schedule a meeting, Outlook shows participants' availability and provides the best available meeting time.

Creating a New Appointment or Meeting

For meeting planning, all CDOB staff can view your availability (free/busy) as indicated on your Outlook calendar. However, no one can view your appointment details unless you have granted them permission through Outlook.

16.5 Wireless Internet Access (Wi-Fi) Services

CDOB provides wireless access at the Chancery Building in Brownsville, San Juan Pastoral Center and Catholic Charities in San Juan. There are two types of wireless access provided; they are:

- CDOBWRL
- CDOB-GUEST

Employees of the diocese are encouraged to use CDOBWRL only while using CDOB Laptops as it provides greater bandwidth and access to network resources. The CDOB-GUEST is used mainly by guests and Employees' Mobile devices.

16.6 Virtual Private Network (VPN)

A virtual private network (VPN) is a connection between computers outside of the CDOB network. The connection uses encryption and other security features to ensure that the data cannot be intercepted by a third-party.

CDOB employees must use the VPN to connect to the CDOB network from outside the CDOB network.

Only CDOB issued laptops are permitted to use the VPN to connect to the CDOB network.

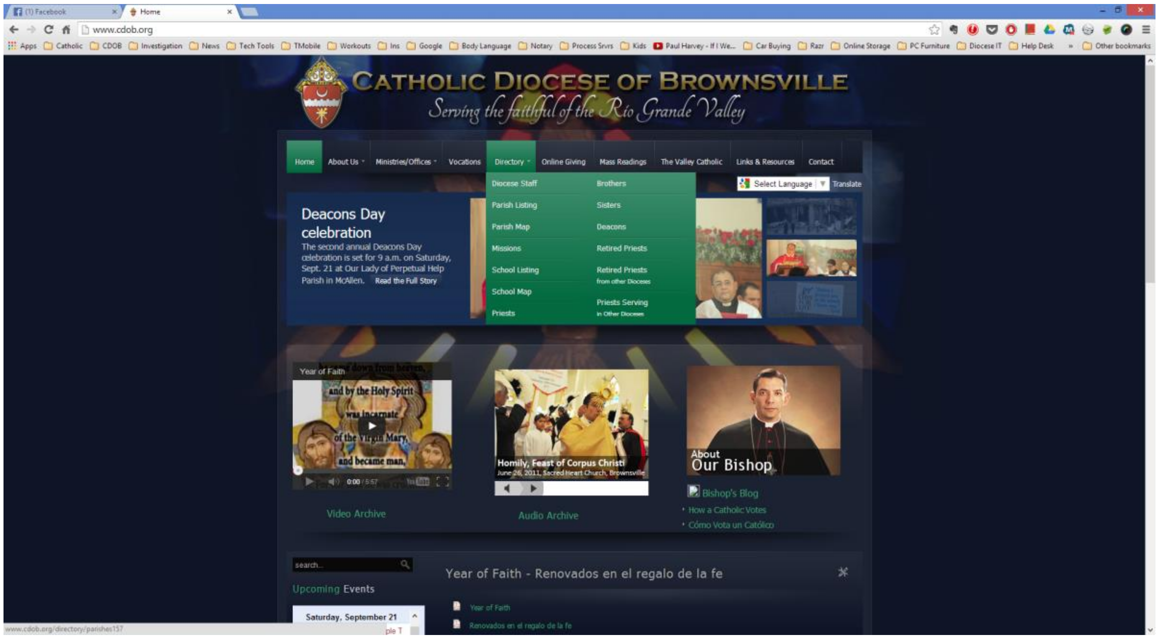
Directors may request installation of the VPN client (software) on CDOB issued laptops for employees needing remote access to the CDOB network.

17 Telephones

17.1 Phone Directory

A phone directory of CDOB personnel is available online through www.cdob.org.

Hover your mouse pointer over Directory and it will expand. You can then select the departments.



Deacons Day celebration

The second annual Deacons Day celebration is set for 9 a.m. on Saturday, Sept. 21 at Our Lady of Perpetual Help Parish in McAllen. Read the Full Story

17.2 Voice Mail (Basic Operations)

All CDOB center employees have voicemail boxes on the CDOB voice mail system. You can access your voicemail box from inside or outside of the CDOB.

To access your voicemail box from your terminal:

Press your Voice Mail Function Key or Press the ”VMsg” button.

To access your voicemail box from outside:

- When your VM picks up, wait for the greeting to start
- Dial # to stop the greeting
- Dial # and your own extension number

17.3 Voice Mail Password

Press your VM Key or push **VMsg**
Push **More> + Optns** + **Sec**
Do one of the following:

- Enter a new security code and push **OK**
- Push **Erase** to erase your security code.
- Push **Back** to exit without changing your security code.

17.4 Greetings

The voicemail system includes three greetings; Internal, External and Temporary. Callers within the CDOB hear your internal greeting. The system plays the external greeting to all other callers. You may also use a temporary greeting if your schedule changes daily and/or for holidays, sick days etc.

If a greeting is not recorded, callers hear a default system greeting stating the extension of the mailbox they have reached. The caller does not hear the name of the individual they are trying to reach and may choose not to leave a message. It is a good idea to always record personal greetings.

17.5 Recording Greetings

Press your VM Key or push **VMsg**
Push **Greet**
Push **Gr1, Gr2** or **Gr3** to select which of the tree available greetings you want to be active.
Do one of the following:

- Push **Lstn** to listen to your greeting (if recorded)
- Push **Rec** to record a new greeting
- Push **Erase** to delete your Greeting (and use the pre-recorded greeting)
- Push **Back** to exit without changing your Greeting

18 IT Resources

Computer Basics
If you are new to the computer, don't worry. We can help. These tutorials will allow you to become comfortable with technology in no time.

OnGuardOnline.gov
OnGuardOnline.gov is the federal government’s website to help you be safe, secure and responsible online.

Office 365 Learning Center
Get started with Office 365 for business. Install, set up, and use Outlook, Word, Excel, PowerPoint, OneNote, and OneDrive for Business on your devices. Learn about Lync, Yammer, Delve, and more, and see how you can be more productive with Office 365.

19 Forms

19.1 CDOB - Return of Property Agreement Form

Employee Full Name: ____

I ___________________________________acknowledge the receipt of the company property listed below along with the value of each item. I understand that each item must be returned to Diocese of Brownsville in good working condition on or before the date of my last day of work at Diocese of Brownsville or at any time as requested by Management. If I do not return the property, Our Moderator of the Curia will determine how to proceed. A copy of this will be placed in my employee file for reference. Diocese of Brownsville may also take all action deemed appropriate to recover or protect its property.

Description	**Serial Number**	**Value**	**Issued Date**	**Returned Date**

Employee Signature: _______________________ Date: ______________________

Witness Signature: _________________________ Date: ______________________

Complete when Employee is separating from Diocese of Brownsville

Employee's last day of work: __________________

The following item(s) were not returned and has been determined to proceed as follows:

____

____

____

____

__________________________ __________________________

HR Director Moderator of the Curia

__________________________ __________________________

Date Date

19.2 Catholic Diocese of Brownsville Information Technology Policies and Procedures Acknowledge Form

I HAVE READ THE CATHOLIC DIOCESE OF BROWNSVILLE'S INFORMATION TECHNOLOGY POLICIES AND PROCEDURES DOCUMENT AND AGREE TO ABIDE BY IT AS CONSIDERATION OF MY CONTINUED EMPLOYMENT WITH THE DIOCESE. I UNDERSTAND THAT ANY VIOLATION OF ANY OF THE ABOVE PROVISIONS OF THESE POLICIES AND PROCEDURES MAY RESULT IN DISCIPLINARY MEASURES, INCLUDING TERMINATION OF MY EMPLOYMENT.

Employee Name____

Employee Signature________________________________ Date______________