Email Encryption

1.   Purpose

The purpose of this document is to explain the steps necessary for sending an encrypted e-mail as well as showing an example of the steps necessary for reading an encrypted message.

2.   Scope

These procedures pertain to all users accessing AoA's 365 platform
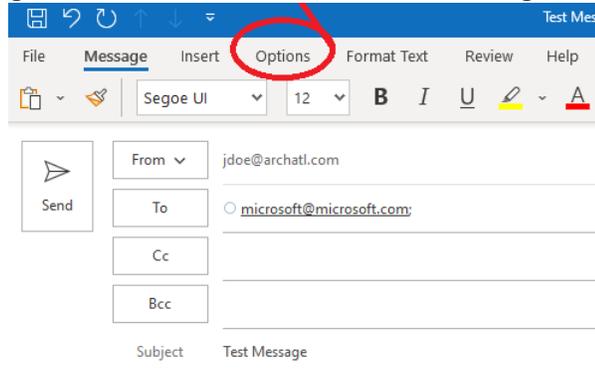
3.   Prerequisites

MS Office 2021 or later.

4.   Responsibilities

It will be the responsibility of AoA's Department of Information Technology to keep these directions updated. Should these procedures require an update, a modification, a correction, etc. – the IT department should be notified by way of the helpdesk ticketing system found at: https://help.archatl.com/
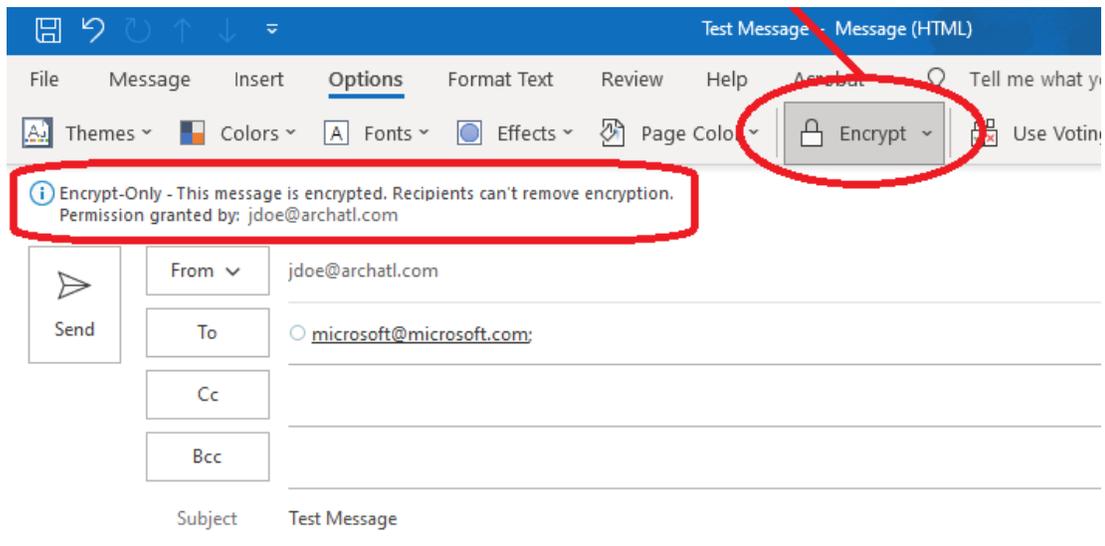
5.   Procedure

1.   Compose your message in Outlook as normal. Before sending, click **Options** ….

This message is a test.

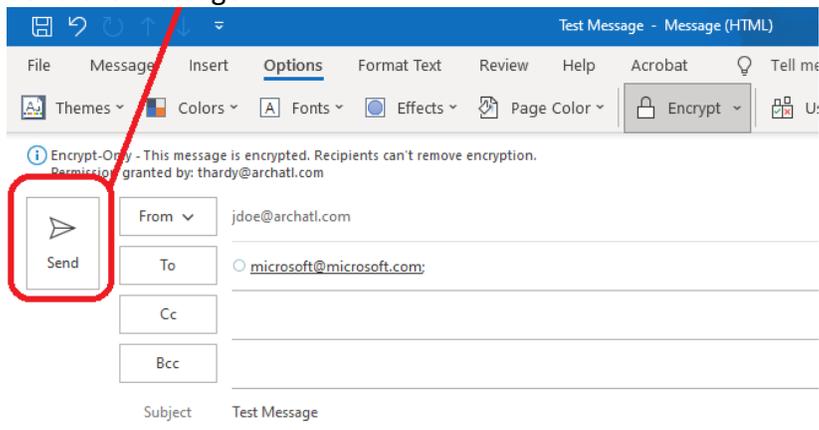2. Next, click the **Encrypt** option (as shown below) and notice the information pop-up displayed that confirms the message will be sent encrypted …
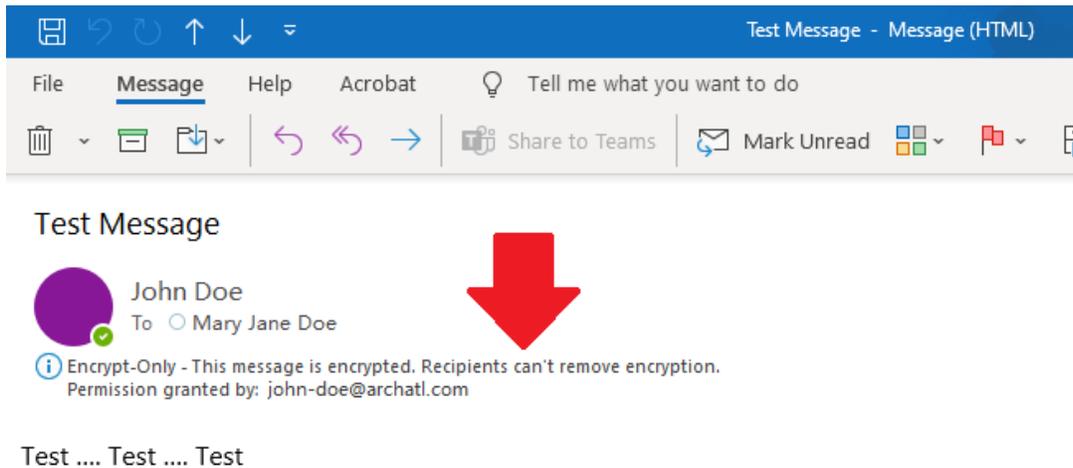

3. **Send** the message …

Depending upon what e-mail platform the receiver of the message is working on, the receipt and access of your message may involve different steps. These instructions cover two scenarios:

- Both Sender and Receiver are on the same (AoA) platform
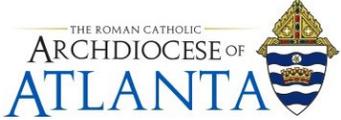- Receiver of the message is on a Gmail platform

Message was Sent to an Archdiocesan Colleague on AOA 365 Platform

Under this scenario, the recipient will receive your e-mail with a notification that the message has been encrypted ….
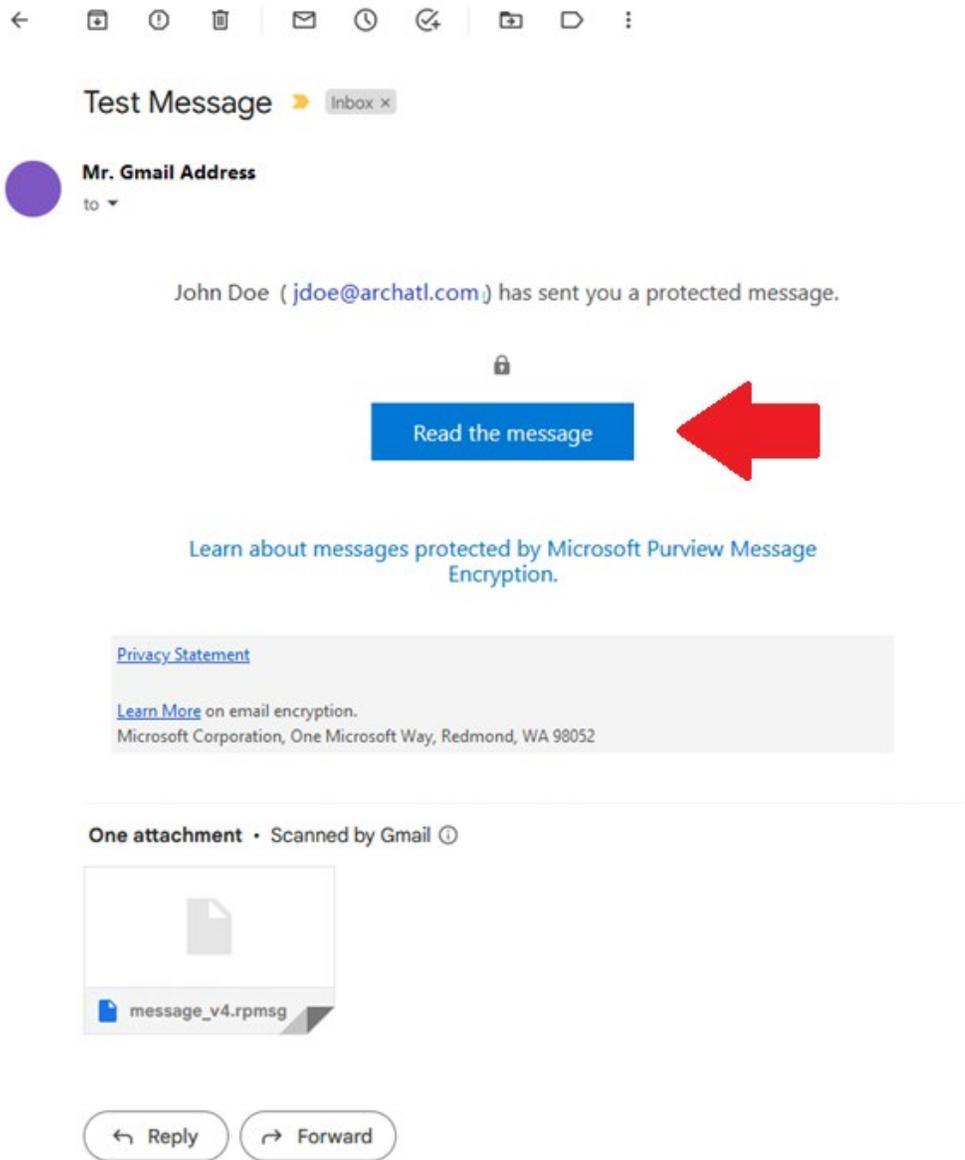

They should be able to access the message without any further steps or procedures

Message was Sent to a Recipient Outside the Archdiocesan 365 Platform (Ex: Gmail)
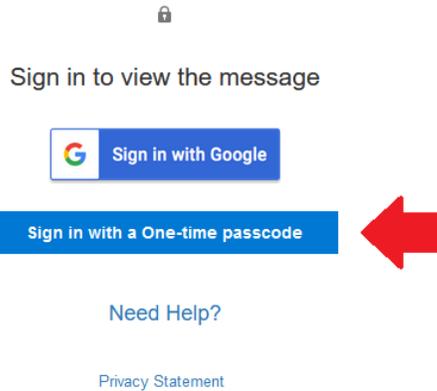
Under this scenario, the recipient will receive <u>a notification</u> of your encrypted email message (see example below). Because the message's contents lie on Microsoft servers and the recipient's e-mail is on another platform (in this example – Gmail), the recipient must click on the **Read the message** option to view the contents of the e-mail ….

Once the recipient has chosen to read the message, they will be taken to a screen similar to that shown below. We recommend that they simply choose to have a 'one-time password' sent to them so that they can use it as the key to open the encrypted message …

john-doe@archatl.com has sent you a protected message

Sign in to view the message

[Sign in with Google]

[Sign in with a One-time passcode]

Need Help?

Privacy Statement

The recipient will then see a screen like the one below. The recipient will need to (**1**) **input the one-time passcode** sent to them and (**2**) click the **Continue** link ….

We sent a one-time passcode to *(recipient @ …..)*

Please check your email, enter the one-time passcode and click continue. The one-time passcode will expire in 15 minutes.

One-time passcode [＿＿＿＿＿＿] 1

☐ This is a private computer. Keep me signed in for 12 hours.

➔ Continue 2

Didn't receive the one-time passcode? Check your spam folder or get another one-time passcode.
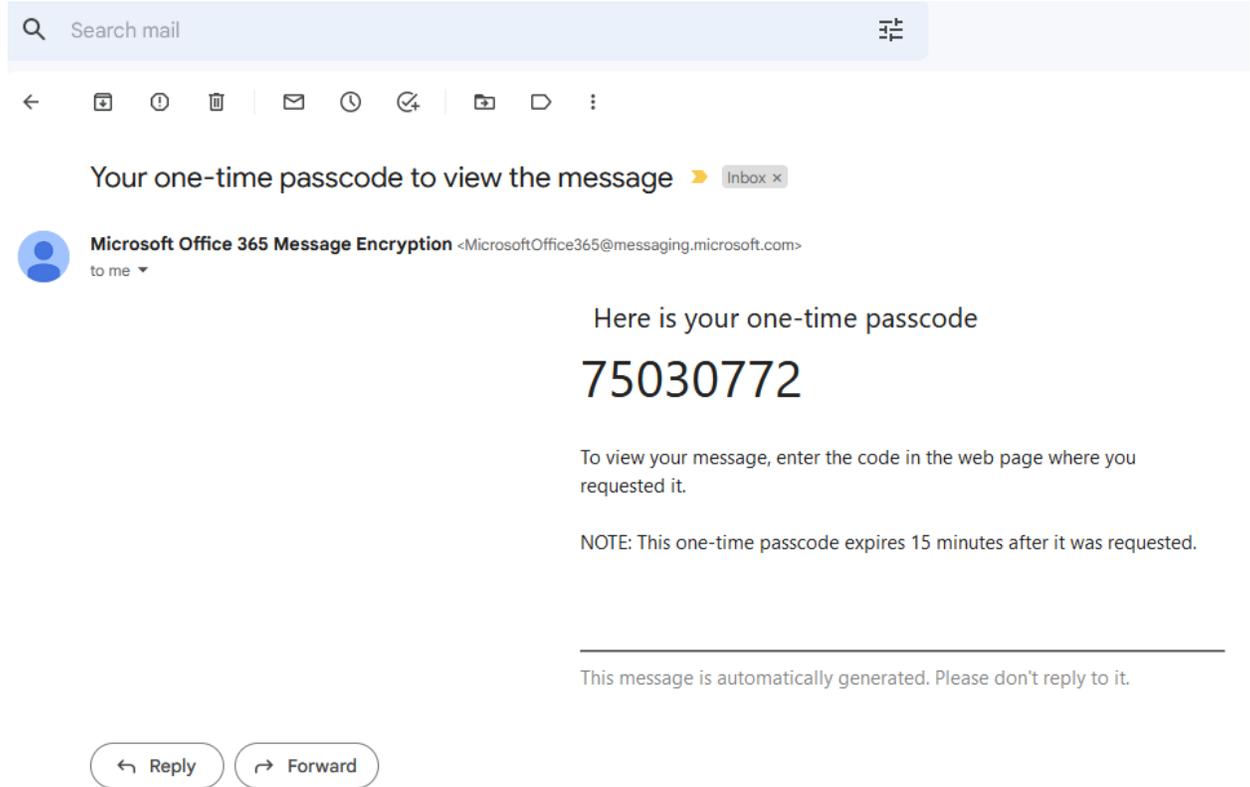
🔒 Message Encryption by Microsoft Office 365

The recipient should see a message like this in their inbox …

☐ ▾   C   ⋮

☐ ☆ ▶ **Microsoft Office 36.**   **Your one-time passcode to view the message** - Here is your one-time passcode 75030772 To view y
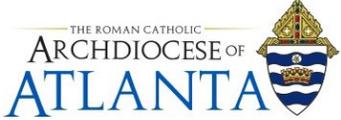
… and when opened, the message should look similar to this:

After going through the 2-step process explained on page 5 (**within 15 minutes of the code being sent**), the actual encrypted message will be retrieved from Microsoft's servers.

Note: This may take a few minutes and the following screen will be displayed …

At this point, the message should be accessible to the recipient …………..

Test Message

John Doe <john-doe@archatl.com>
Today, 2:04 PM

Encrypt: This message is encrypted. Recipients can't remove encryption.

Encrypted Content

6.   References

A library of procedures such as this may be found at AOA IT Dept.'s Knowledgebase which can be accessed on the Helpdesk site at: https://help.archatl.com

7.   Definitions

None.