GIG CYMRU NHS WALES Bwrdd Iechyd Prifysgol Caerdydd a'r Fro Cardiff and Vale University Health Board	**Reference Number: UHB 558** **Version Number: V.1** **Next Review Date: 11.11.2028** **Previous Trust/LHB Reference Number: n/a**

Procedure for Sending Emails Externally

Introduction and Aim

Cardiff and Vale University Health Board (the UHB) is required to send a significant volume of external communications that may contain confidential data. The UHB's position is that confidential information should only leave the UHB's network via secure means.

During the COVID-19 pandemic it became clinically necessary for medical professionals to send sensitive data to email addresses outside the Cardiff and Vale University Health Board network. This has remained an important part of delivering UHB services and aligns with Principle 7 of the Caldicott Principles, which states: "The duty to share information can be as important as the duty to protect patient confidentiality".

This procedure has been developed to support UHB staff to comply with the UK General Data Protection Regulation (UK GDPR) by ensuring the safe transfer of any sensitive data. This is especially pertinent to data transferred outside of the UHB's network.

Objectives

The objectives of this procedure are to:

- Provide staff with a framework to help them understand how to maintain data security when sending external emails.
- Educate staff on external data transfers through the Secure File Sharing Portal (SFSP) or the use of Transport Layer Security (TLS) Assurance.
- Explain the process for authorised exceptions using authorised generic mailboxes, or through individual clinical decision.
- Explain common mistakes made that result in data breaches and how to avoid them.

Scope

This procedure applies to all of our staff in all locations, including those with honorary contracts.

Equality Impact Assessment	An Equality Impact Assessment has not been completed because this procedure supports the overarching Information Governance Policy for which an EHIA has already been undertaken.
Documents to read alongside this Procedure	Information Governance Policy Data Protection Act 2018

	UK GDPR The Caldicott Principles Generic Mailbox Management – Appendix A Information Governance on the Use of Email and Generic Mailboxes to Communicate with Patients – Appendix B Generic Mailbox Set Up – Appendix C
Approved by	Digital & Infrastructure Committee
Accountable Executive or Clinical Board Director	Director of Digital Health & Intelligence
Author(s)	Head of Information Governance and Cyber Security

Disclaimer

If the review date of this document has passed please ensure that the version you are using is the most up t date either by contacting the document author or the Governance Directorate.

Summary of reviews/amendments			
Version Number	**Date of Review Approved**	**Date Published**	**Summary of Amendments**
1	11.11.2025	15.01.2026	Content previously included within Management of Policies, Procedures and Other Written Control Documents Policy. It has been updated to include any changes in arrangements and the new style of written control documents.

CONTENTS

1. SCOPE

The scope of this procedure is all sensitive data leaving the UHB's network via email. This includes patient-sensitive data, staff-sensitive data, and business-sensitive data.

2. PERSONAL DATA

Information that relates to an identified or identifiable living individual is considered personal data – this includes both patient and staff information.

In determining whether an individual is identifiable, staff need to consider whether any party (including the UHB) is able to directly or indirectly single out or identify an individual, either by using that information alone or in combination with any other information that is likely to come into their possession.

Identifiers include but are not limited to a name, surname, initials, age, a home address, postcode, an email address, race, ethnic origin, genetic data, health data, NHS number, hospital number, a study number, any other unique identifier, among many others. However, it is also necessary to consider each dataset in its totality to determine whether any combination of data items within it could be used to link back to an identifiable individual.

Staff members should understand the difference between pseudonymised data and anonymised data. Data that has been attributed a pseudonym or that can be indirectly linked back to an individual is classed as pseudonymised data. Significantly, this remains personal data and within the remit of data protection legislation.

Anonymised data is data that has been processed to remove any personally identifiable information and thus **cannot** be linked to a living individual. Where data is truly anonymised, it falls outside of data protection legislation and no security measures are required.

2.1 Patient and Staff Data

The UHB has made provision for certain non-sensitive patient data to be communicated via UHB email accounts. More detailed guidance and technical support on this process is available in this document's appendices.

All staff should be aware that sensitive patient data that, if disclosed, could cause harm or embarrassment to a patient (e.g. sexual health data) can be sent via the UHB's SFSP but cannot be sent externally via a generic UHB email account.

Staff data should be securely protected in the same way as patient data.

3. BUSINESS-SENSITIVE DATA

Business-sensitive data concerns any data that is sensitive to the commercial functions of the UHB. This could include trade secrets or data that may harm commercial interests if publicly disclosed. Staff should understand that this type of data must be sent securely to ensure operational security.

4. PROCEDURE STATEMENT

4.1 UK GDPR Principles

It is the duty of UHB staff members to be aware of UK GDPR principles which are taught through Information Governance (IG) training provided on the Electronic Staff Record (ESR) online portal. This procedure aims to ensure further compliance with the UK GDPR principles and creating norms for secure data transfer outside the UHB network in line with the aforementioned principles.

4.2 External Data Transfers

The UHB maintains that external data transfers should only take place under certain circumstances. External data transfers should be supported by either the SFSP or through TLS Assurance.

TLS should be used for frequent transfers as it establishes a permanent connection to external addresses. This means that emails are sent securely using encryption. With this additional level of assurance, it is now permissible to send and receive sensitive information to and from organisations on the TLS list (available here: TLS Assurance) from your @wales.nhs.uk email. Staff members should refer to this list if they are unsure whether an email address is secure. If an address is not on the list then the SFSP should be used for information transfer.

The SFSP is available to all NHS Wales employees who wish to send sensitive information to another Trust or Health Board or third-party organisation securely – a genuine business need is required for its use. The SFSP should be used for infrequent or one-off data transfers.

These two methods are the most effective and secure ways of transferring data outside of the UHB's network and should be the first port of call when transferring data.

4.3 Other Means of Transferring Data

While the SFSP and TLS are the preferred method of securely transferring data, there are authorised exceptions that may apply when correct security measures are taken to avoid data breaches.

Generic mailboxes can be used to ensure the transfer of data outside the UHB as well as if there is an individual clinical decision based upon the need to access the relevant data. In these instances, the identity of the recipient must be verified before the transfer can begin. This can be achieved by seeking relevant photographic ID (e.g. a passport or a driving licence), and proof of address (e.g. a utility bill or a bank statement). There are restrictions to the information that can be transferred through the use of generic mail boxes. The use of generic mailboxes for this purpose must be in accordance with the generic mailbox guidance documents – please see Appendix A, B, and C.

Password-protected emails are a common method of data transfer and can be used when appropriate. It is worth noting that the SFSP and TLS are a more secure

method of transfer, but if there is a genuine need, password protection is a viable option.

Sending the password for accessing a document in the same email as the protected document will render the protection null. This is a frequently made mistake when trying to send messages externally. Should your message be intercepted, the protected document can then be accessed by the interceptor.

5. TRAINING

5.1 ESR Training

Staff members are required to complete their IG mandatory training module which will provide an understanding of how to lawfully process personal data and how to ensure patient confidentiality. To deepen their understanding, staff members are also encouraged to read the Caldicott Principles and the All Wales Email Use Policy.

6. IMPLEMENTATION

The implementation of these requirements should be made a part of standard practice for all staff who regularly send sensitive data externally.

6.1 Implementation of the SFSP and TLS Assurance

To implement the SFSP and TLS Assurance, staff should contact the Cyber Security Department and the IG Department. Their email addresses can be found here:

- Cyber Security: cv.imt.security@wales.nhs.uk
- Information Governance: cav.ig.dept@wales.nhs.uk

The SFSP will be installed as a desktop icon by Cyber Security.

The IG Team will also ask for a TLS Assurance form to be completed in order to establish a secure connection with the external organisation.

7. RESPONSIBILITIES

It is the responsibility of all members of staff to avoid these frequent errors listed below.

7.1 Carbon Copy and Blind Carbon Copy

Breaches often occur due to the incorrect use of Carbon Copy (CC) and Blind Carbon Copy (BCC). For non-sensitive communications, senders may wish to use the BCC function for mass emails which might not require a response and to hide the email addresses of the recipient in order to protect privacy. Recipients may have a legitimate interest to keep their email address private due to the associated cyber risks if their address is disclosed outside of the UHB.

Be aware that the BCC function, while sometimes useful, presents a real risk to personal information if used incorrectly and is not enough on its own to properly protect people's personal information. Staff must therefore use secure alternatives like the SFSP when sending personal data outside of the UHB’s secure network.

The ICO has published guidance for sending bulk communications by emails, available here.

7.2 Correct Email Addresses

Data breaches can occur due to the incorrect email address being typed out by the sender. This will negate any security measures put in place. Where possible, staff must endeavour to copy and paste email addresses rather than typing freehand to ensure that the correct email address is being used. It is also beneficial to double check the email address before sending as an added level of security.

7.3 Generic Mailboxes

Staff members should use generic mailboxes where possible if there is a need to send clinical information through unsecure methods. Patients should be informed of the risks and should be consulted when having their data shared through unsecure methods. This should be as a last resort.

A generic email account should have automated responses informing the recipient of the times the inbox is monitored as well as any other relevant information (e.g. where to redirect emails possibly sent to the wrong department).

7.4 Email Subject Lines

Staff members should ensure that no patient data is contained within the subject line of any correspondence unless the message is secure. Data breaches often occur when staff members reply to emails with patient data appearing in the subject line – most frequently the patient's name and date of birth. If you are sent an email with patient data in the subject box, it must be amended to remove any personal data before replying to the sender.

8. REVIEW

9. APPENDICES

APPENDIX A

Generic Mailbox Management

Patient safety

It is important that **patients** are made aware and are reminded regularly that clinic mailboxes are:

- Not to be used for communicating emergencies
- Not monitored 24/7
- Should not be used to send sensitive clinical information about patients

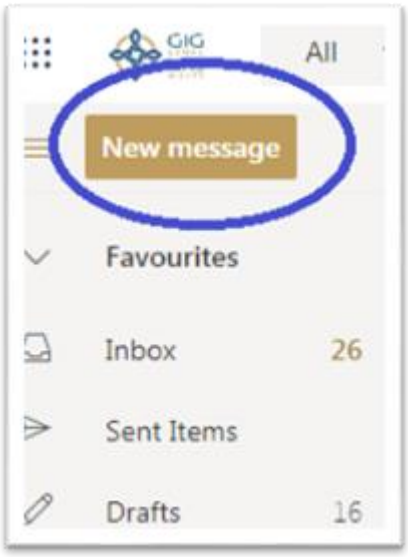
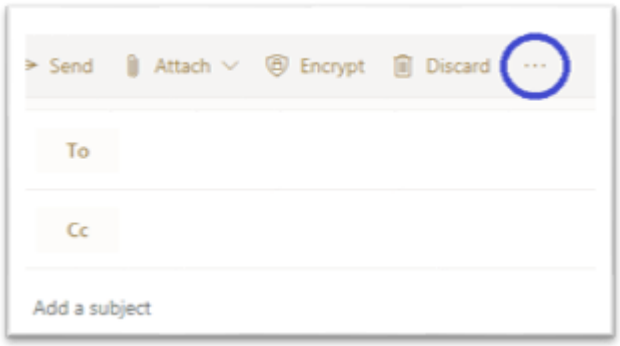
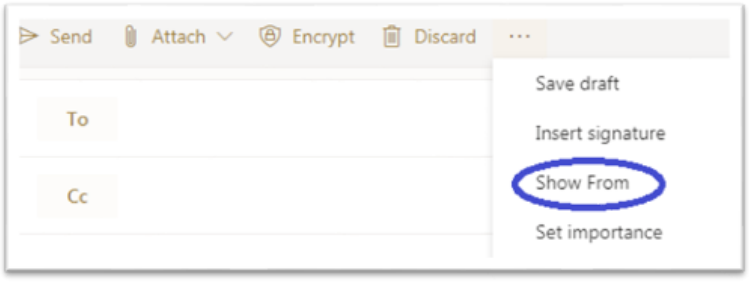
This can be done by setting up a standard Out of Office which will automatically be sent to any patient writing to the mailbox – see page 4 of this guide

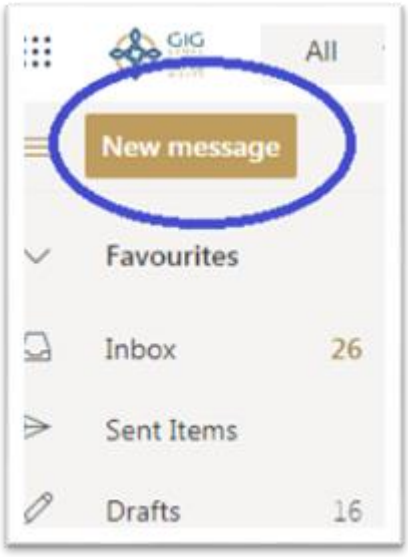
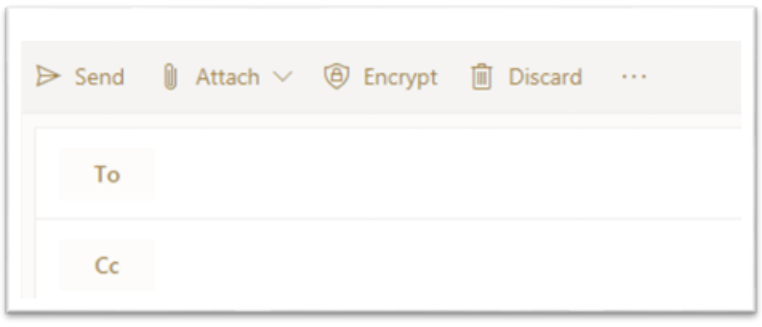
Mailbox management

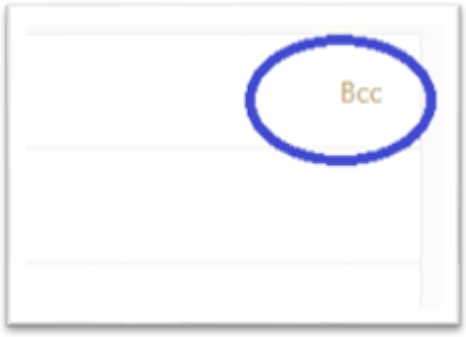
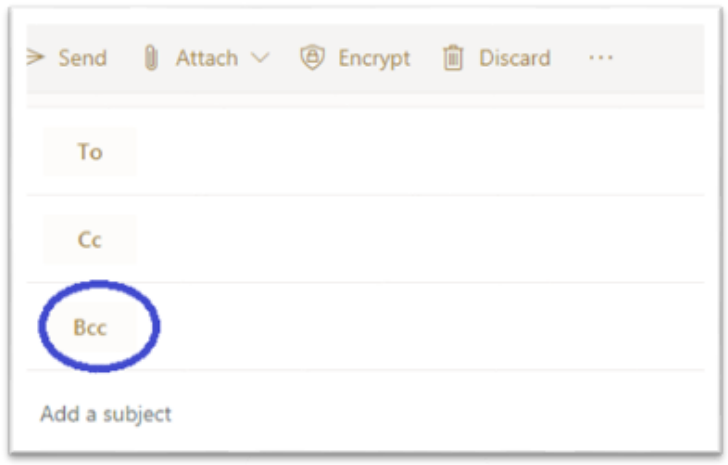
It is also important that **clinics document/ create SOP** to cover the following

- Identify how mailboxes will be monitored, how patient queries are managed and are responded to
- Have an agreed frequency that mailbox contents will be reviewed
- Are used in accordance with the IG guidance provided

How to send a message

2	Click new message in Outlook Email.	
3	In the header of the email, select 3 dots.	
4	Select Show From This will enable you to select the correct mailbox is shown as the sender. I.e. not your individual email address, but the shared mailbox address.	

5	Select the relevant email address. Note: First time in selecting a send from mailbox, you will need to search for it from the directory, then going forwards, it will appear as a drop-down option having been selected in the past.	
How to use the Blind Carbon Copy (BCC) Function		
	Why use BCC?	Using the Bcc field will ensure email addresses are **hidden from all recipients.** This is especially important if you are writing to more than 1 patient at a time. Using the Bcc field will **prevent recipients from REPLYING TO ALL** on the distribution list. Replies will go to the sender only and not to every person in the distribution list. Some staff members do not wish patients to have their work personalised email so this will prevent personal details going to the patients
	Click new message	
	The message header will appear.	

	Click on Bcc (this is on the top right-hand section of the message header)	
	This will open the Bcc field in the message header. Input recipient email addresses into the Bcc field	
Out of Office		
	Using an Out of Office message on your inbox	Consider using the out of office function for communicating key information to patients and as a disclaimer. 1. Remind patients to include their name, date of birth, address and NHS CRN/UNIT number when emailing the generic mailbox, and if they haven't done so, ask them to resend the email. 2. Disclaimer example: Your health and care professionals will not be constantly monitoring emails you send. **PLEASE NOTE**: This is not for use in an emergency. For urgent medical care or advice call 0300 10 20 247. In a case of serious injury or illness which may be life-threatening, call 999. Your care professionals may also have given you advice on what to do in an emergency. https://cavuhb.nhs.wales/news/campaigns/cav-247/ This mailbox is not monitored 24/7.

APPENDIX B

Information Governance on the use of email and generic mailboxes to communicate with patients

The UHB has authorised the use of generic mailboxes as a digital means of communicating with patients for non-sensitive information via email to patients for example to signpost or communicate 'general' health data and information such as:

- Treatment/care plans
- Appointments
- Non-sensitive results

Sensitive data such as results and clinical images in relation to the following **cannot** be sent via email.

- Mental health data
- Sexual health data
- HIV status

Use of generic email addresses is subject to the following guideline.

Sending information to patients as part of a consultation

- Email addresses should be obtained directly from the patient during consultation (whether face-to-face, telephone or virtual)
- Once collected, the email address should be validated against the email address held in the relevant patient admin system (e.g., PAS, Paris etc). If emails don't match you need to seek sufficient information from the patient that confirms the correct identity.

Responding to patients contacting a generic email account

- If disclosing information, services will need to be satisfied they are communicating with the correct individual. The following data is **required** as a means of confirming the patient's identity:
  - NHS number/CRN (at the discretion of the service if not provided)
  - Name
  - Address
  - Phone number
  - DOB
- If publicising a generic mailbox (for example putting the mailbox address on your clinic webpages or letters to patients), the relevant communication **must** include the following statement:
- 'In providing us with your email address, we may use this for future communication with you, as per our Patient Privacy Policy. We can only be responsible for emails held on our network and not the security of email providers for those who contact us.'

Responding to carers contacting a generic email account acting on a patient's behalf

- If disclosing information, services will need to be satisfied the carer has consent or appropriate authority to act on the patient's behalf. This is in addition to the data required to confirm the patient's identity.
- Services may opt to keep a register of carers authorised to act on a patient's behalf.

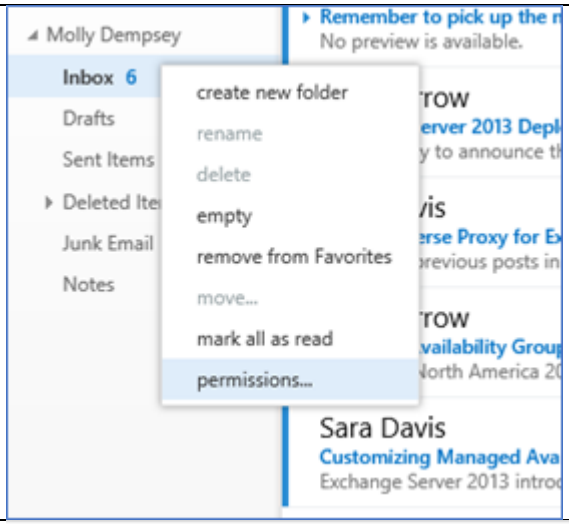
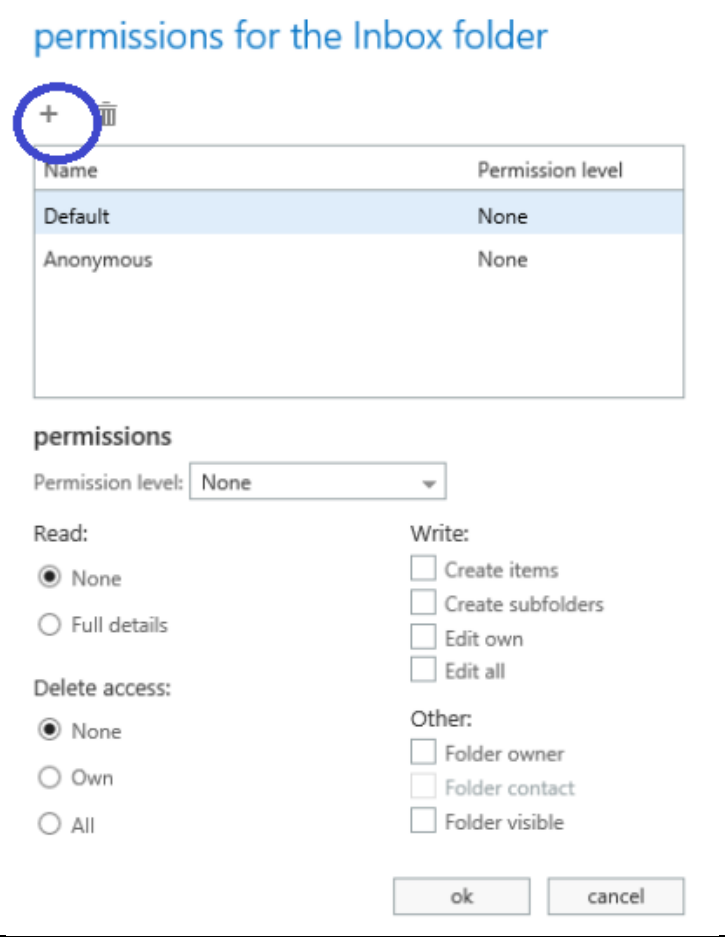
If there are any concerns about the authenticity of the user, no information should be disclosed.

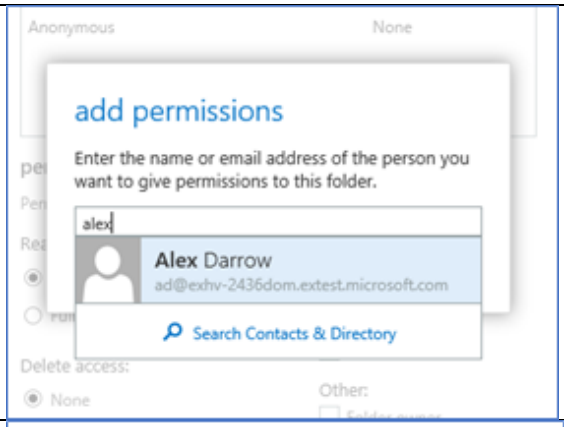
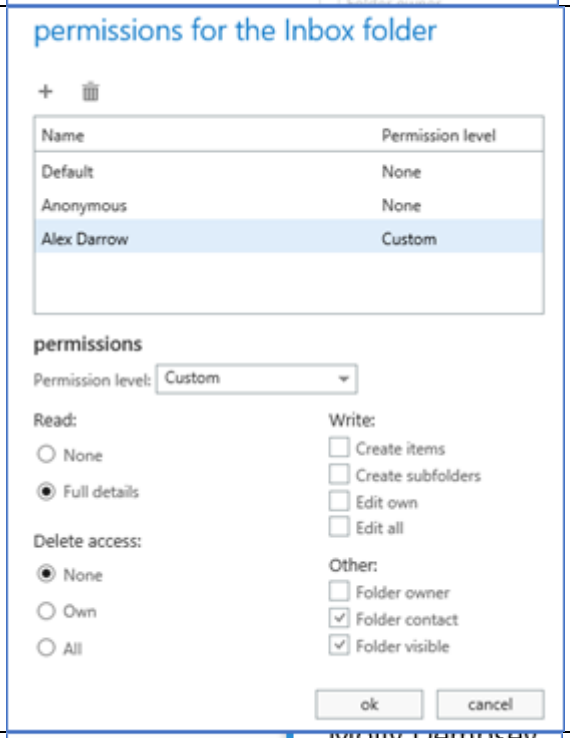
If the communication includes any data of clinical significance, this data will need to be retained in the patient's clinical record and not in Outlook or any other drive. Can it be loaded to Com? Or other systems used? Or would it need printing?

If you have any doubts or require advice, please contact the CAV Information Governance Department: Cav.ig.Dept@wales.nhs.uk

APPENDIX C

Generic Mailbox Set Up		
1	Users need to complete the online request on the helpdesk page	Shared Mailbox Request Form (office.com) Digital Portal for a shared mailbox and the permissions are set automatically
2	Once the mailbox is created	IT will e-mail those selected as account admins with instructions as below
3	Add mailbox to Outlook.	**For Outlook on your desktop** if you use this version, you just need to restart Outlook and the mailbox will appear on the left-hand menu list but right at the bottom of the list as an extra mailbox. If you use **Outlook online**, follow these instructions below. **When in Outlook Online**, within the left-hand section there is a word 'Folder' (Above the word 'Inbox') Right click over the word 'folder' and select 'Add Shared Folder' then start typing the name of the mailbox and it will appear. Select the mailbox and click ADD. Then it will be added as an additional mailbox on the left-hand side under your main inbox folders
4	Add mailbox users and set user permissions.	

5	Right click shared mailbox Inbox and select permissions.	
6	This brings up the folder permissions dialogue box. Click the plus sign (+) at the top left of the dialog box.	
7	Type the name of the user you wish to add to the shared mailbox.	

			
8	Choose permission settings in the drop-down menu or create custom permissions. Click OK.		
9	If you wish to add permission to view any folder other than Inbox, there is one more step. After setting permissions for the folder that you wish to share, click on your mailbox's root folder ("Molly Dempsey") and grant permissions to that as well. Click OK.