Beginner's Guide to Sending or Sharing Sensitive Information via Microsoft 365

1. Understand What Counts as Sensitive Information

Before sending, identify if your email contains:

- Personal data (e.g., names, addresses, National Insurance numbers)
- Financial data (e.g., bank details, payroll information)
- Confidential business plans, contracts, or intellectual property
- Client/customer information
- Credentials or access details

If yes, extra care is required before hitting "Send". Take a look at the following security options before proceeding. If you are a Cosurica customer call our Support Team for advice.

---

2. Use Microsoft 365 Message Encryption (OME)

Microsoft 365 includes built-in encryption features. Here's how to use them:

Encrypt an Email in Outlook (Desktop or Web):

1. **Compose a new message.**
2. Go to the **Options** tab.
3. Click **Encrypt**.
4. Select one of the following:
    - **Encrypt-Only** – email is encrypted, but recipients can forward it.
    - **Do Not Forward** – adds both encryption and restrictions on forwarding, printing, and copying.

Tip: Use "Do Not Forward" for the most sensitive content.

---

3. Add Sensitivity Labels (if your organisation has them)

Sensitivity labels apply data classification and protection policies. This functionality is available with Microsoft 365 Business Premium and some Enterprise plans, or as add-ons for Enterprise plans which don't include this functionality as standard.

How to Apply:

- When composing an email in Outlook, look for the **"Sensitivity"** dropdown in the toolbar.
- Select a label such as **"Confidential", "Restricted", or "Internal Use Only"**.

Labels may:

- Automatically encrypt the message
- Watermark content
- Prevent copying or forwarding

The availability of these options is governed by your Microsoft 365 licence. Your Microsoft 365 Admin configures these options if they are available to you, and the options available will vary by organisation.

If you're a Cosurica customer and you're not sure what options you have, give our Support Team a call.

---

4. Double-Check Recipients and Attachments

Before sending:

- **Verify the email addresses** — especially important if you have autofill enabled.
- Use **@mentions** carefully in sensitive emails.
- **Confirm attachments** are the correct versions and free from hidden metadata.
- Consider using **OneDrive links** instead of attaching sensitive files directly.
- If you must attach sensitive documents directly to an email, ensure they are password protected as an absolute bare minimum and don't communicate the password to open the document by email!
- If the option to use Information Rights Management is available to you, use it to **Protect** the document, so access is limited only to specific people. You should limit recipients to read only wherever possible, so they can't copy or print the data in the file (which they might do to get round security and share the info with someone you haven't given access to).

---

5. Use Safe Links for Shared Files

When attaching or sharing files via OneDrive:

- Click **Share**, then:
    - Choose **"Specific People"** to limit access.
    - Disable editing if not needed.
    - Set an expiration date or password.

These links:

- Provide better access control
- Allow revocation if needed
- Improve visibility through audit logs

It's possible to follow the above steps to share files via Sharepoint too, but this can be problematic. Doing so may be affected by or interfere with access permissions already in place. If you are a Cosurica customer considering this option, please call our Support Team for advice.

---

6. Enable Read Receipts or Delivery Notifications

While not foolproof, enabling delivery and read receipts can add confidence that your message was received.

In Outlook:

- Go to **Options**
- Tick **"Request a Delivery Receipt"** or **"Request a Read Receipt"**

Note: The recipient must approve sending a read receipt, so there's no guarantee you'll get a Read Receipt!

---

7. Avoid Sending from Mobile Whenever Possible

While mobile apps are convenient, they often hide security features like:

- Encryption options
- Sensitivity labelling
- Detailed recipient previews

Important – You really should be using desktop or web Outlook for all sensitive communications, because the options available in mobile apps tend to be very limited

---

8. Report Mistakes Immediately

If you send sensitive information to the wrong recipient:

- **Recall the message** (if possible) via Outlook, but do be aware this is rarely effective!
- **If you can't recall the message send an email to the unintended recipient requesting they delete the email** immediately
- **Notify your IT/Security team*** immediately
- **Use Microsoft 365 Compliance Center** for data loss tracking and response, which is normally handled by your IT team or IT provider*.

***If you're a Cosurica customer all you need to do is phone our Support Team straightaway and we'll help you!**

---

9. Use Multifactor Authentication (MFA)

Ensure MFA is enabled on your Microsoft 365 account. This:

- Reduces the risk of unauthorised access
- Is a baseline requirement for sending and storing sensitive data
- Where possible use an authentication app or device for MFA rather than receiving verification codes via SMS or phone (for a greater level of security).

Important: If you're a Cosurica customer and you're unsure if you have MFA enabled call our Support Team for advice.

---

10. Stay Educated

Security tools evolve. Attend internal training if available, watch for phishing warnings, and read Microsoft 365 security updates regularly.

Unfortunately, people tend to be the weakest link in your security armour, because they are easily distracted, often in a rush to get the job done and can react emotionally rather than logically when put under pressure.

We recommend the **KnowBe4** cyber security awareness training platform as this product is designed specifically for small to mid-size organisations. KnowBe4 delivers all the training your people need to avoid being caught out by the social engineering tactics now widely used by cybercriminals to get around technical security measures.

If you'd like to know more about KnowBe4, or you would like a demo, please give our sales team a call on 01535 358161.

Sending Sensitive Data Checklist

Task	Done?
Identified sensitive content?	☐
Applied encryption/sensitivity label?	☐
Double-checked recipients and attachments?	☐
Used secure links instead of raw attachments?	☐
Used a trusted device (not mobile)?	☐
Enabled MFA and kept it active?	☐