



COLLECTING EMAIL IN A FORENSICALLY SOUND WAY

A practical guide and checklist for lawyers and investigators

TABLE OF CONTENTS

WHY THIS MATTERS	3
BEFORE YOU COLLECT ANYTHING	3
LEGAL HOLDS (WHAT TO THINK ABOUT)	3
COLLECTING EMAIL IN A DEFENSIBLE WAY	4
CHAIN OF CUSTODY AND DOCUMENTATION	4
COMMON RISKS TO WATCH FOR	5
EMAIL COLLECTION – SHORT CHECKLIST	5

WHY THIS MATTERS

Email is often central evidence. How it is preserved and collected can be just as important as what it contains. Poor handling can lead to allegations of spoliation, missing metadata, or doubts about authenticity. This guide is not about “how to click the buttons”, but about **what you should be thinking about** to keep the evidence defensible.

BEFORE YOU COLLECT ANYTHING

1. Be clear on scope and purpose

- Confirm **why** the email is being collected (litigation, regulatory response, internal investigation).
- Identify:
 - Who the custodians are (people whose mailboxes matter)
 - The relevant date range
 - Whether attachments, calendar items, deleted emails, or shared mailboxes are in scope
- Write this down. Vague scope leads to over-collection or missed evidence.

2. Decide who should do the collection

- Email collection should be done by:
 - Internal IT following a clear legal instruction, or
 - An external forensic provider
- Avoid ad-hoc collections by business users or managers “just exporting what seems relevant”.

3. Preserve first, collect second

- Preservation stops data changing.
- Collection is copying data out.
- Preservation should happen **as soon as litigation is anticipated**, not when proceedings formally start.

LEGAL HOLDS (WHAT TO THINK ABOUT)

A legal hold ensures relevant email is not deleted or altered by users or automated retention rules.

Key points for lawyers and investigators

- Confirm that a legal hold has been applied **before** collection begins.
- Check that it covers:
 - All relevant mailboxes (including shared or former employee mailboxes)
 - The correct date range
- Understand that:
 - A legal hold does not export email
 - It preserves content in the background, even if a user deletes it

Practical checks

- Ask IT or your provider to confirm, in writing:

- When the hold was applied
 - Which custodians it applies to
 - Whether any data may have been lost before the hold went on
- Keep a copy of the legal hold notice and any acknowledgements.

COLLECTING EMAIL IN A DEFENSIBLE WAY

What “forensically sound” means in practice

You are aiming to show that:

- The original data was not altered
- The collection was repeatable and explainable
- Metadata (dates, senders, recipients, attachments) was preserved

Good practice checklist

- Use **official Office 365 tools** designed for legal discovery, not manual drag-and-drop.
- Export email in a format that preserves structure and metadata (commonly PST).
- Do not:
 - Open, forward, or selectively save emails from the live mailbox
 - Ask custodians to self-collect their own email
- Record:
 - Who performed the collection
 - When it was done
 - Which mailboxes and date ranges were included
 - The search terms or filters used (if any)

CHAIN OF CUSTODY AND DOCUMENTATION

If the email ends up before a court, someone may ask: “How do we know this wasn’t changed?”

Simple but critical steps

- Keep a clear log showing:
 - Where the data came from
 - Who handled it
 - Where it was stored
- Store collected email:
 - In a secure, access-controlled location
 - Separately from working copies used for review
- Avoid renaming, re-saving, or re-packaging original exports without recording it.

COMMON RISKS TO WATCH FOR

- Late legal holds: email deleted before preservation cannot be recreated.
- Over-collection creates cost, delay, and review risk.
- Under-collection: missing custodians or date ranges can be more damaging.
- IT acting without legal direction: technical actions without legal framing are hard to defend later.

EMAIL COLLECTION – SHORT CHECKLIST

1. Trigger and scope

- ☐ Has litigation, a regulatory matter, or a serious investigation been identified?
- ☐ Are the relevant custodians, date range, and issues clearly defined in writing?

2. Preserve first (legal hold)

- ☐ Has a legal hold been applied in Office 365 **before** collection?
- ☐ Does the hold cover all relevant mailboxes (including shared and ex-employee accounts)?
- ☐ Has IT or the provider confirmed when the hold started and what it covers?

3. Control who collects

- ☐ Is collection being done by IT or a forensic provider, not the custodian?
- ☐ Are ad-hoc exports, forwarding, or “saving emails to a folder” prohibited?

4. Defensible collection

- ☐ Are approved Office 365 eDiscovery tools being used (not manual copying)?
- ☐ Is email being exported in a format that preserves metadata (e.g. PST)?
- ☐ Are search terms, filters, and date ranges documented?

5. Chain of custody

- ☐ Is there a record of who collected the data, when, and from where?
- ☐ Is the original export stored securely and kept read-only?
- ☐ Is access to the collected data restricted and logged?

6. Sanity checks

- ☐ Have any gaps, errors, or missing data been identified and noted?
- ☐ Is the collection ready to be explained to a court if required?