15 June 2026,

Subject: Technical Response Regarding Alleged Use of Email Draft Folders to Avoid Public Records Requests

Dear Mayor and Members of Council,

At the Town's request, Advanced Data & Network Solutions has reviewed the technical concern that Town staff may be using Microsoft 365 email draft folders to communicate with one another in a way that avoids public records requests.

This letter provides a technical assessment only. Advanced Data can not be considered an independent forensic auditor for this matter. This is not a legal opinion regarding North Carolina public records law, records retention requirements, or the Town's obligations in responding to any particular records request. Such determinations should remain with the Town's Attorney and appropriate Town records officials.

Request Received from Town Management

On Wednesday, June 10 2026, Advanced Data & Network Solutions received the following request from the Interim Town Manager:

> *"We have had a citizen attend the last 2 Council meetings and complain about the Town's Planning Staff. He has accused them and past staff of utilizing draft folders on projects, so they can correspond with each other and avoid any public records requests, since it is only a draft document. He has also stated that these draft documents are later modified or items are deleted prior to it becoming a final draft or final email. He has requested Council to authorize an independent, third party audit of the email metadata and the draft folders of certain employees. Is this something that can be determined, and if so, what is the process and a potential cost? I need to be able to provide Council with an update on his complaint."*

The purpose of this letter is to respond to that technical question: whether this type of activity can be evaluated, what such a review would involve, and whether the requested independent forensic audit appears reasonable based on the Town's Microsoft 365 environment.

Summary

The allegation appears to involve a technique sometimes referred to as "foldering." In general terms, this would mean that two or more people avoid sending emails and instead communicate by accessing the same mailbox draft folder, editing draft messages, and then deleting or changing those drafts before anything is formally sent.

While this concept has appeared in popular entertainment and has been discussed in some investigative contexts, it is technically unlikely based on the controls currently in place within the Town's Microsoft 365 environment.

The Town's Microsoft 365 environment uses several important safeguards:

1. **Named user accounts**

60 Ravenscroft Dr. ♦ Asheville, NC 28801
828-285-8882 office ♦ 828-281-2772 Fax
WWW.ADNSOLUTIONS.COM

- Each employee uses an individual Microsoft 365 account rather than a general shared account for normal business use.

2. **Multi-factor authentication**
   - Users are required to verify their identity with more than just a password.
3. **Conditional access and security controls**
   - The environment is configured to restrict or prevent logins from unusual locations or unusual sign-in patterns, consistent with commonly accepted cybersecurity practices.
4. **Centralized Microsoft 365 audit and security records**
   - Microsoft 365 maintains records related to sign-ins, mailbox access, permissions, administrative changes, and other relevant activity, subject to licensing, configuration, and retention limits.

For the alleged activity to occur, staff would generally need to share their personal credentials, share access to a multi-factor authentication method, improperly delegate mailbox access, use an authorized shared mailbox for an improper purpose, and/or compromise an account or device. Each of those scenarios is unusual and would be contrary to current cybersecurity policies.

In short, while no technology provider can claim that a misuse scenario is absolutely impossible, the alleged practice is technically unlikely in the Town's current Microsoft 365 environment and would typically create indicators that could be reviewed.

Explanation of the Alleged Method

The concern being raised can be illustrated this way:

```
Alleged "Foldering" Method

Person A logs into mailbox X
        ↓
Person A writes a message but does not send it
        ↓
The message remains in the Drafts folder
        ↓
Person B logs into or accesses the same mailbox
        ↓
Person B reads, edits, or deletes the draft
        ↓
No ordinary sent/received email appears between Person A and Person B
```

This scenario is much more plausible in an environment where multiple people share the same username and password, where multi-factor authentication is not used, and where audit logging is limited or absent.

That is not how the Town's Microsoft 365 environment is structured.

A more accurate view of the Town's environment is:

```
Town Microsoft 365 Model

Employee A → Employee A account → Employee A mailbox
Employee B → Employee B account → Employee B mailbox
Employee C → Employee C account → Employee C mailbox

Controls:
- Multi-factor authentication
- Unusual-login restrictions
- Named-account access
- Mailbox permission controls
- Microsoft 365 audit and security records
```

These controls do not make misuse impossible, but they substantially reduce the likelihood of the alleged method being used successfully or routinely without detection.

What Can Be Reviewed

A technical review can look for indicators of the alleged activity. For example, it can examine available Microsoft 365 data to determine whether there are signs of:

- unusual account sign-ins;
- logins from unexpected locations;
- blocked or challenged sign-in attempts;
- mailbox access by someone other than the mailbox owner;
- unusual mailbox delegation or permission changes;
- shared mailbox access;
- unusual deletion patterns;
- relevant administrative changes;
- signs of account compromise.

This type of review can provide useful information and may help determine whether there is any technical basis for the allegation.

However, a technical review cannot responsibly prove that something has never happened at any point in the past. Any review is limited by available logs, Microsoft licensing, retention periods, system configuration, and the specific users and dates included in the review.

The appropriate technical question is not:

> *"Can we prove this has never happened?"*

A more appropriate question is:

> *"Do the available Microsoft 365 records show indicators of shared mailbox access, suspicious sign-ins, unusual permissions, abnormal deletion activity, or account compromise for the relevant users and time period?"*

That is a question that can be reviewed.

Cost and Scope Considerations

A broad independent forensic audit would likely be expensive. Based on the type of work being requested, an independent third-party forensic review could reasonably cost approximately $30,000 or more, depending on scope.

Cost would be affected by:

- number of employees reviewed;
- number of mailboxes reviewed;
- date range;
- whether employee devices must be examined;
- whether deleted-data recovery is requested;
- whether Teams, OneDrive, SharePoint, or mobile devices are included;
- whether legal chain-of-custody procedures are required;
- whether a formal expert report or testimony is expected.

There is a significant difference between a limited Microsoft 365 technical review and a full forensic investigation.

Limited Technical Review	Full Forensic Audit
• Microsoft 365 configuration	• Independent forensic firm
• MFA and conditional access settings	• Legal chain of custody
• Sign-in records	• Mailbox collection
• Mailbox permissions	• Device imaging
• Available audit logs	• Deleted-data recovery
• Written technical summary	• Expert report
	• Possible testimony
	• Broader legal support

Absent specific technical indicators of wrongdoing, a full independent forensic audit may be disproportionate to the allegation.

Recommended Path Forward

We recommend a measured, evidence-based approach.

First, the Town should consult with the Town Attorney regarding any public records, preservation, or legal obligations.

Second, if Council wishes to evaluate the technical concern, the Town should define a limited review scope, including:

- the employees involved;
- the relevant mailboxes;
- any shared mailboxes to be included;
- the date range;
- the systems to be reviewed;
- the specific question to be answered.

Third, Advanced Data & Network Solutions can assist with a limited review of available Microsoft 365 configuration and audit information. That review could include MFA status, conditional access controls, unusual sign-in activity, mailbox permissions, shared mailbox access, administrative changes, and available audit records.

If that review identifies suspicious indicators, Council could then consider whether a broader independent forensic audit is justified.

Conclusion

Based on the Town's current Microsoft 365 environment, the alleged use of email draft folders as a covert method of routine staff communication appears technically unlikely.

The Town uses named Microsoft 365 accounts, multi-factor authentication, restrictions against unusual login activity, mailbox permission controls, and Microsoft 365 audit and security records. These safeguards are consistent with commonly accepted cybersecurity practices and materially reduce the practicality of the alleged method.

At the same time, it is important not to overstate what technology can prove. A technical review can look for indicators of suspicious activity within available records, but it cannot prove a universal negative for all users and all time periods.

Our recommendation is that the Town first conduct a limited, well-scoped Microsoft 365 technical review before committing public funds to a broad independent forensic audit. If that review identifies evidence of suspicious access, unusual mailbox activity, or account compromise, the Town can then evaluate whether a formal independent forensic investigation is warranted.

Respectfully submitted,

Advanced Data & Network Solutions

60 Ravenscroft Dr. ♦ Asheville, NC 28801
828-285-8882 office ♦ 828-281-2772 Fax
www.adnsolutions.com