



KATHLEEN JENNINGS
ATTORNEY GENERAL

DEPARTMENT OF JUSTICE
820 NORTH FRENCH STREET
WILMINGTON, DELAWARE 19801

CIVIL DIVISION: (302) 577-8400
CRIMINAL DIVISION: (302) 577-8500
FAMILY DIVISION: (302) 577-8400
FRAUD DIVISION: (302) 577-8600
DIVISION OF CIVIL RIGHTS & PUBLIC TRUST: (302) 577-5400
FAX: (302) 577-2610

Office of the Attorney General of the State of Delaware

Attorney General Opinion No. 26-IB34

June 17, 2026

Via Email

Shannon Marvel McNaught
shannon.marvel@doverpost.com

RE: FOIA Petition Regarding the Town of Dagsboro

Dear Ms. McNaught:

We write in response to your correspondence, alleging that the Town of Dagsboro violated Delaware's Freedom of Information Act, 29 *Del. C.* §§ 10001-10008 ("FOIA"). We treat this correspondence as a Petition for a determination pursuant to 29 *Del. C.* § 10005 of whether a violation of FOIA has occurred or is about to occur. As discussed more fully herein, we determine that the Town violated FOIA by failing to demonstrate its withholding of access to the requested records was permitted by FOIA.

Background

On May 25, 2026, you submitted a FOIA request to the Town of Dagsboro, seeking "all emails between police and email addresses ending in @fbi.gov and @ice.dhs.gov between Jan. 1, 2024 and May 25, 2026."¹ A day later, the Town denied this request in its entirety. The Town asserted that under 29 *Del. C.* § 10002(o), "records compiled for law-enforcement purposes, investigatory files, intelligence information, and documentation where disclosure could interfere with active law enforcement proceedings, techniques, or jeopardize public safety" were not public records, and the communications between local police and federal law enforcement agencies regarding operational or investigatory matters fall within these protections.² In addition, the Town

¹ Petition.

² *Id.*

stated, to the extent any such communications exist, information between these federal entities and local police is subject to federal confidentiality protocols, information-sharing agreements, and restrictions precluding disclosure. The Town also stated it does not have a centralized system capable of filtering, isolating, and extracting emails across multiple independent employee accounts; reviewing individual accounts to generate a new synthesized compilation of data would constitute creating a new record, which FOIA does not require. Doing such a search, the Town argues, would impose an unreasonable administrative and legal burden. Finally, the Town asserted that “forcing manual extraction from workstations utilized for law enforcement networks violates the security protocols governed by the Delaware Criminal Justice Information System (‘DELJIS’), which limits system access to authorized users for legitimate criminal justice actions.”³

This Petition followed, contesting the Town’s denial. You argue that not all the requested emails relate to investigations, and any exempt investigatory information can be redacted. You allege that the Town’s claims asserting federal confidentiality restrictions prohibit disclosure and manual extractions from workstations violate DELJIS security protocols are both false. In addition, you state that police agencies seeking communications for a FOIA request typically request those communications from the Delaware Department of Technology and Information (“DTI”), but you ask this Office to clarify the agency from which FOIA submitters should request police emails.⁴

On June 4, 2026, the Town, through its legal counsel, responded to your Petition. The Town argues that these emails are categorically exempt pursuant to the investigatory file exemption. The Town disagrees that the DTI should execute a backend search and deliver a master data list to the Town, arguing that the DTI does not have custody of the emails, “nor does it act as an administrative processor for local police departments.”⁵ The Town also asserts that requesting this data would constitute creation of a new record because the Town “has individual, user-level Microsoft Outlook profiles” and does “not possess a centralized, keyword-search infrastructure.”⁶ The Town argues that it would be an undue burden to require a “micro-agency with zero administrative or IT staff to request a bulk, unfiltered backend data dump from an external host – and then forcing untrained active-duty officers to manually review thousands of lines of raw text.”⁷ The Town states that the police department has a total of five sworn officers and no staff or internal IT department, and forcing active duty officers to attempt highly technical data manipulation and legal sorting severely disrupts the core emergency operations of the agency.

³ *Id.*

⁴ This general question is not appropriate for the FOIA petition process, which is limited to addressing allegations of FOIA violations. 29 *Del. C.* § 10005(e).

⁵ Response.

⁶ *Id.*

⁷ *Id.*

In addition, the Town argues that complying with this request risks noncompliance with the DELJIS and CJIS rules. The Town states that every terminal used by the police department interfaces directly with the DELJIS network. The Town asserts that under DELJIS statutes and the corresponding FBI CJIS Security Policies, workstation and account access is restricted to authorized individuals for legitimate criminal justice purposes; additionally, the Department Policies 321.4 and 807.6.1 strictly prohibit officers from sharing passwords or entering other employees' accounts. The Town argues that "forcing staff to manually log into and harvest backend data from separate user profiles creates an unmanaged network vulnerability and a reportable 'Security Incident,' risking the immediate revocation of the department's access to vital national and state criminal databases."⁸ Finally, the Town contends that an automated backend extraction based on a trailing domain character string would expose highly sensitive internal law enforcement communications, victim data, and confidential personnel information to officers who do not have the right to view them directly, which violates the "principle of least privilege" under state networking laws.⁹

Discussion

Delaware's FOIA law "was enacted to ensure governmental accountability by providing Delaware's citizens access to open meetings and meeting records of governmental or public bodies, as well as access to the public records of those entities."¹⁰ FOIA requires that citizens be provided reasonable access to and reasonable facilities for the copying of public records.¹¹ The public body has the burden of proof to justify its denial of access to records.¹² In certain circumstances, a sworn affidavit may be required to meet that burden.¹³

Judicial Watch, Inc. v. University of Delaware provides that Section 10005(c) "requires a public body to establish facts on the record that justify its denial of a FOIA request."¹⁴ "[U]nless it is clear on the face of the request that the demanded records are not subject to FOIA, to meet the burden of proof under Section 10005(c), a public body must state, under oath, the efforts taken to determine whether there are responsive records and the results of those efforts."¹⁵ In this case,

⁸ *Id.*

⁹ *Id.*

¹⁰ *Judicial Watch, Inc. v. Univ. of Del.*, 267 A.3d 996, 1004 (Del. 2021).

¹¹ 29 Del. C. § 10003(a).

¹² 29 Del. C. § 10005(c).

¹³ *Judicial Watch, Inc.*, 267 A.3d at 1008-1012.

¹⁴ *Id.* at 1010.

¹⁵ *Id.* at 1012.

while the emails may be mostly protected by the investigatory files exemption, the Town has not demonstrated how all requested emails are exempt on their face so the Town must determine whether there are responsive records.¹⁶

The Town's remaining arguments are unavailing. Searching and producing emails, or parts thereof, does not constitute creation of a new record.¹⁷ FOIA states that requests "for e-mail records shall be fulfilled by the public body from its own records, if doing so can be accomplished by the public body with reasonable effort."¹⁸ "If the public body determines that it cannot fulfill all or any portion of such request, the public body shall promptly request that its information and technology personnel or custodians provide the e-mail records to the public body."¹⁹ Before requesting emails from the IT staff or custodian, the public body must provide an itemized cost estimate for any charges expected to be incurred in retrieving the emails. In this case, the Town asserts that the DTI does not have custody or administrative access to the requested emails and this request constitutes a burden to the police department with five officers, and no internal IT or administrative staff. As FOIA does not contain exceptions for the burdens it imposes on smaller municipalities or departments with limited resources, the request cannot be denied on that basis.

In addition, the Town's assertion that searching and reviewing emails with sensitive content would violate DELJIS, federal rules, or other security protocols is not sufficiently specific. FOIA contemplates that public bodies have the capabilities to review, produce, and redact emails with sensitive or exempt information without running afoul of their other requirements. As such, we find that the Town violated FOIA by failing to meet its burden of demonstrating that access to the requested records in their entirety was appropriately denied under FOIA. To remediate this violation, we recommend that the Town, in compliance with the timeframes set forth in Section 10003, review its responsive records and supplement its response with any additional records, responses, or information, if appropriate under FOIA. If authorized costs are anticipated, a cost estimate may be provided, as set forth in Section 10003.

¹⁶ Section 10002(o)(3) exempts "[i]nvestigatory files compiled for civil or criminal law-enforcement purposes including pending investigative files, pretrial and presentence investigations and child custody and adoption files where there is no criminal complaint at issue."

¹⁷ *Vanella v. Duran*, 2024 WL 5201305, at *9 (Del. Super. Dec. 23, 2024) ("Furthermore, FOIA requires access to public records 'regardless of the physical form or characteristic by which such information is stored, recorded or reproduced.' It would defeat the letter and spirit of FOIA to not use a computer system in a manner that can isolate and produce only the troopers' names. FOIA makes no 'distinction between records maintained in manual and computer storage systems.' Producing easily disclosable information stored in a computer system does not require the creation of a new record.").

¹⁸ 29 Del. C. § 10003(i).

¹⁹ *Id.*

Conclusion

Based on the foregoing, we conclude that the Town violated FOIA by failing to demonstrate its withholding of access to the requested records was permitted by FOIA.

Very truly yours,

/s/ Dorey L. Cole

Dorey L. Cole
Deputy Attorney General

Approved:

/s/ Patricia A. Davis

Patricia A. Davis
State Solicitor

cc: Gregory A. Morris, Town Solicitor