United States
Consumer Product Safety Commission

NUMBER:	Directive 0731
SUBJECT:	Managing Official Agency Email
DIRECTIVE OWNERS:	Office of the General Counsel (OGC), Division of Information Access (GCIA); Office of Information and Technology Services (EXIT)
EFFECTIVE DATE:	February 7, 2024

---

1. PURPOSES.

The purposes of this directive are to:

- make users aware of acceptable and unacceptable uses of CPSC's email system;
- ensure users avoid conducting official business using non-CPSC email systems;
- outline CPSC's email retention policy and requirements; and
- ensure compliance with the National Archives and Records Administration's (NARA) General Records Schedule (GRS) 6.1, Capstone, sections 10 and 11.

2. SCOPE.

This Directive applies to all CPSC email account holders and users, all email systems owned or operated by CPSC, and all CPSC email records. Note: Union officials' records about union business are not federal records and as such are not subject to the records retention portions of this directive.

3. AUTHORITIES.

a. 44 U.S.C. Chapter 31 (Records Management/Federal Agencies)

b. 44 U.S.C. Chapter 33 (Disposal of Records)

c. 36 C.F.R. Chapter XII, Subchapter B (Records Management)

d. Email and Other Electronic Messages Managed under a Capstone Approach, GRS 6.1. CPSC Records Management Directive

e. CPSC Information Systems Rules of Behavior.

4. POLICIES.

a. Email Accounts and Uses

CPSC email account holders are issued official cpsc.gov email addresses upon onboarding. From that time until their departure, CPSC email account holders should use only their cpsc.gov email accounts when using email for CPSC official business.

CPSC email account holders must use an official CPSC device to conduct agency business and transmit agency records when teleworking. Absent exceptional circumstances as described below, CPSC email account holders may not forward non-public CPSC data or documents to personal email accounts.

b. Privacy Expectations

CPSC email account holders should have no expectation of privacy when using Commission-provided email systems. Certain CPSC officials have the authority to access any email created, stored, sent, or received on CPSC's systems when there is a legitimate government purpose for such access.

Emails may also be subject to public release under the Freedom of Information Act (FOIA), reviewed and produced in response to civil discovery, subpoenas, or other legally authorized inquiries, or voluntarily disclosed by CPSC.

c. Acceptable Use

The use of email on CPSC's automated information systems is intended to support CPSC's mission. All CPSC information systems that permit the sending and receipt of email are federally owned or licensed and are provided to CPSC staff and contractors to conduct official business.

It is prohibited to use CPSC email systems for illegal or unauthorized purposes, including but not limited to:

- copyright infringement;
- libel, slander, or defamation;
- fraud;
- prohibited political activity;

- harassment or intimidation;
- forgery;
- impersonation;
- soliciting for schemes;
- terrorism and related activities;
- illegal drug or weapon activity;
- sharing confidential CPSC information;
- commercial purposes or "for-profit" activities;
- gambling;
- chain letters or unauthorized mass mailings;
- viewing or sharing pornographic or sexually explicit material;
- computer tampering (intentional dissemination of viruses/malware); and/or
- endorsing any product, service, or enterprise, except as authorized.

d. Use of Non-CPSC Email Systems for Official CPSC Business is Prohibited

CPSC email account holders may not use non-CPSC email systems to conduct government business, unless such email is copied or forwarded to a CPSC email system within 20 days.[1] Absent exceptional circumstances that render authorization impracticable, the use of a non-CPSC email system to conduct government business must be authorized by an immediate or second-level supervisor. Examples of exceptional circumstances include, but are not limited to, continuity of operations (COOP) activities or other activities necessitated by the temporary unavailability of CPSC email systems.

e. Limited Personal Use

CPSC email account holders may use CPSC email systems to send infrequent, short personal messages if such activity does not reduce employee productivity, interfere with

[1] 44 U.S.C. § 2911(a).

official business, or cause congestion, delay, or disruption of service to any government system or equipment. For more information about personal use of government technology, consult Directive 0720.1, *Limited Personal Use of CPSC Information Technology Resources*.

f. Personally Identifiable Information and Confidential Business Information

CPSC email system users must redact or remove any confidential information, including sensitive personally identifiable information (PII) or confidential business information (CBI), when sending email or email attachments to parties who are not authorized to receive that confidential information.

It is the policy of the CPSC to scan outgoing emails sent to external addresses for the possible inclusion of certain sensitive PII categories. Emails identified as potentially containing sensitive PII are not sent; instead, the attempted sender will receive an automatic email with guidance on secure transmission.

To protect the agency's systems and data, staff must report any suspected or confirmed breaches of PII or CBI to the Chief Privacy Officer (privacy@cpsc.gov) and the Computer Security Incident Response Team (CSIRT) (csirt@cpsc.gov) as soon as they become aware of an occurrence.[2]

g. Email Storage

Official email systems are not the appropriate vehicle for storing official documents. Storing records consistent with the requirements of CPSC's official records systems is crucial for compliance, accountability, disaster recovery, knowledge management, and overall data security. It helps the agency streamline operations, protect sensitive information, and maintain a clear, auditable trail of communication and decision-making processes. Any official records sent or received through email must be saved to a relevant, official CPSC application.

All items received by or saved in CPSC email systems, including personal email, will be retained for the periods specified below. Users who wish to avoid government retention of their personal communications should not use CPSC email and messaging systems for personal communications.

h. Email Retention Policy

CPSC follows the National Archives and Records Administration's (NARA) "Capstone" approach to managing and retaining emails. Generally, senior officials' emails are

[2] 44 U.S.C. § 3554(b)(7).

"permanent" records (*i.e.*, saved forever), whereas the emails of all other email account holders, including staff and contractors, are "temporary" records and routinely deleted after seven years from the date of creation.

More information on Capstone, including which electronic messages fall under the schedule and how long an agency must retain them, are found in NARA's general records schedule (GRS) 6.1, 010 - 011. *See* GRS 6.1, 010-011, *Email and Other Electronic Messages Managed under a Capstone Approach* (Jan. 2023).

1) Email Retention Policy for Capstone Officials

   Capstone Officials, defined by NARA as "senior officials designated by account or position level," includes the Chair and Commissioners, as well as the most senior policy-making officials at CPSC.[3] All emails to and from current and former Capstone officials are retained permanently. At the end of the Capstone official's term with the agency, those items are accessioned (*i.e.*, legal title in the records is transferred) to NARA.

2) Email Retention Policy for Non-Capstone Officials

   For any current and former staff and contractors not designated Capstone officials, all items in their CPSC email accounts will be retained for seven years from the date of creation. Seven years from the date the record is created, the record will be deleted unless it must be preserved because of a litigation hold or another reason approved by the Executive Director.

i. Preserving Emails in Response to Litigation Holds

The Office of the General Counsel and the Office of Compliance and Field Operations (EXC), may place a hold on any records related to anticipated or pending litigation, which is commonly referred to as a "litigation hold." OGC and/or EXC will issue agency-wide and targeted litigation hold notifications via email, outlining records custodians' preservation duties. These notifications will include language describing how to preserve the records, including responsive emails. OGC and/or EXC will notify records custodians once the hold is lifted.

j. Policy Violations

In accordance with the agency's Rules of Behavior, failure to adhere to the policies listed above may result in disciplinary action, retraction of system privileges, and/or personal

[3] The current list of Capstone officials is available on EXIT's SharePoint page, at Capstone Method - Capstone Officials.xlsx.

liability for unlawful use of CPSC email systems.

5. **Effective Date.**

   This directive becomes effective on the date signed by the Chair.

Alexander Hoehn-Saric

Digitally signed by Alexander Hoehn-Saric
Date: 2024.02.07 09:23:36 -05'00'

Alex Hoehn-Saric
Chair

Date