Template Whistleblower Confidentiality Policy[1]

Purpose: The purpose of this document is to ensure sufficient protections for the confidentiality of sensitive whistleblower information as the **[MEMBER OFFICE OR COMMITTEE]** (hereinafter, "Office") engages with whistleblowers from the public and private sectors to support the Office's oversight work **[AND CONSTITUENT SUPPORT FUNCTIONS]**.

Requirements: The House Code of Official Conduct mandates confidentiality protections for whistleblower information, and House Information Security Policy requires heightened security protections for information provided in confidence or with restrictions on its use.[2]

Information provided to the Office by a constituent, source, or whistleblower (hereinafter, "whistleblower") may fall within the ambit of this policy. As a best practice, the Office will assume that whistleblower information is sensitive and should be handled and used with caution.

Note: This Information Security Policy relates solely to information that is **not** classified. Policy and procedures for matters relating to classified material or communications are **not** contained in this document. Consult the Office of House Security for specific guidance concerning the lawful handling of classified information. Consult the Office of the Whistleblower Ombuds for guidance on the laws and processes that protect classified whistleblowing disclosures.

1. **Decision maker(s).**

   The **[MEMBER/CHAIR/RANKING MEMBER]** has responsibility for making the key decisions affecting the Office's collection, retention, and use of all information related to whistleblower matters.

2. **Principal contact.**

   The principal contact for overseeing and implementing this policy is the Office's **[INSERT TITLE]**.

3. **Office staff cybersecurity requirements.**

   All users of House information resources and systems must comply with applicable House information security policies and guidance. These requirements include completing

---

[1] This document has been informed by:

1. The E-Government Act of 2002, sect. 208, P.L. 107-347, 116 Stat. 2899 (Dec. 17, 2002);

2. Office of Management and Budget Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003);

3. Fair Information Practice Principles reported in Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress, Federal Trade Commission (May 2000); and

4. House Information Security Publication, Guidelines for Identifying, Handling, and Protecting House Sensitive Information, HISPUB 10.1 (Sept. 4, 2025).

[2] House Code of Official Conduct, H.R. Res. 5, 119th Cong. (2025) (enacted).; House Information Security Policy, Protection of Sensitive Information, HISPOL 10.0 (May 31, 2024).

required training and using only House-approved devices, software, and accounts. Users must also connect through the House Virtual Private Network (VPN), as required.

4. **Purpose for collecting information.**

   The Office will collect information from whistleblowers to further the Office's oversight goals **[AND SUPPORT CONSTITUENT SERVICES]**. Whistleblowers may be constituents or individuals seeking the Office's assistance with remedying misconduct or seeking assistance for reprisal they face for reporting misconduct.

5. **Intended use for the information collected.**

   Information will be collected to assess the validity and extent of the alleged misconduct; to support a decision whether to pursue, or not to pursue the matter; to guide investigation and oversight of the alleged misconduct; and to inform legislation to address the alleged misconduct. Additionally, information may be collected to support whistleblowers facing retaliation.

6. **Confidentiality protections for individuals making protected disclosures.**

   The identity of, and personally identifiable information about, an individual making a protected disclosure to the Office under federal whistleblower law will be protected from public disclosure under the House Code of Official Conduct, Clause 21. Limited exceptions exist, such as obtaining the whistleblower's advance written consent.[3]

   Applicability of Clause 21. The determination of whether a disclosure is protected under a federal law is ultimately a matter of law and fact.[4] The Office will liberally construe the application of law to the facts of whistleblower matters brought to its attention to err on the side of treating matters as falling under the protections of Clause 21.

   Anonymous whistleblowers. The office may receive disclosures anonymously, where the identity of the whistleblower is unknown and where there may be no way to respond or communicate with them. Nonetheless, the disclosure may include personally identifiable information, and the information should be handled with care.

7. **Heightened Information security protection for sensitive information.**

   Information provided to the Office in confidence or with restrictions on its use is considered **sensitive information** and will be provided heightened electronic, physical, and operational security protections in accordance with House information security policy.[5]

8. **Information to be collected.**

   Examples of information typically collected follow.

---

[3] House Code of Official Conduct, H.R. Res. 5, 119th Cong. (2025) (enacted).

[4] For an overview of specific whistleblower sectors and issues, see the compendium of fact sheets and Congressional Research Service reports at https://whistleblower.house.gov/fact-sheets.

[5] Protection of Sensitive Information, House Information Security Policy (HISPOL) 10.0 (May 31, 2024).

a. Involving a whistleblower:
    i. Name, age, address, phone number
    ii. Other personally identifiable information (i.e., Privacy Act)
b. Involving their employment:
    i. Employer, job location, department, work history
c. Involving their disclosure:
    i. Substance of the disclosure
    ii. Timelines of the alleged misconduct or disclosures
    iii. How the alleged misconduct came to the whistleblower's attention
    iv. Documentary evidence (i.e., emails, photos, notes of phone calls, other records)
    v. Metadata associated with documentary evidence (i.e., track-changes and author information embedded in a file, geo-location data embedded in a photo)[6]

9. Information considered personally identifiable or sensitive.

On a case-by-case basis, any or all the information identified in paragraph 8, above, may require the confidentiality protections of the House Code of Conduct and the heightened electronic, physical, and operational security protections of House information security policy. The Office will liberally construe the boundary of which information will be protected under this policy, but as a baseline, the following will be considered **sensitive (whistleblower) information**:

a. Identifying characteristics of a whistleblower (i.e., name, address)
b. Information relating to a whistleblower who provided information in confidence or with restrictions on its use. This may include the unique set (or subset) of facts, even without names or other commonly identifiable elements, that encompasses a disclosure of misconduct or retaliation because it may be sufficient to identify the whistleblower[7]
c. Information provided in confidence or with restrictions on its use

10. Notice and consent procedures.[8]

a. As information is collected from whistleblowers, they will be given notice of their right to confidentiality under the House Code of Official Conduct. Here is a sample script of what may be said:
    - *If you choose to remain confidential, the Office will respect your wishes and do everything within its power to protect your confidentiality.*
    - *Offices are generally prohibited from publicly disclosing your identity without*

[6] See House Office of Cybersecurity: Cybersecurity 101 — What You Need to Know, for background on metadata and how to remove it from various types of files, https://housenet.house.gov/page/5468.
[7] This may be applicable even for anonymous whistleblowers, where the Office does not know the identity of the source.
[8] Applicable for whistleblowers that have shared a means for the Office to communicate with them.

your prior written consent, but there may be factors beyond our control that we will discuss, for example, surveillance technology and legal limitations.

- *There can be no guarantee of confidentiality. You may need to take additional precautions, such as camouflaging your digital footprint or unique facts, having a plan for the possibility of your confidentiality being breached, and seeking experienced legal counsel.*

b. Whistleblowers will be informed of the Office's confidentiality and information security practices, as captured in this document, and will be granted the following rights:

   i. Right to have the integrity and security of the information protected in accordance with the requirements and best practice standards set by the House

   ii. Right to review the information in advance of its use by the Office

   iii. Right to update the information to correct errors and remove identifiable information

   iv. Right to object to the use, including sharing, of the information

11. Confidentiality and information security procedures and controls.

Whistleblower information that requires confidentiality and heightened information security protections will have the following safeguards:

a. All staff will be educated on their responsibility for protecting sensitive whistleblower information, including the mandate to maintain whistleblower confidentiality, in accordance with this policy, the House Code of Official Conduct, and the relevant House information security policies

b. Access is restricted to authorized staff designated as having a need to know[9]

c. Contractors and vendors must execute a non-disclosure agreement prior to access

d. Electronic information will be communicated, processed, shared, and stored on official House equipment (including authorized removable media[10]) and House-contracted technology service providers, using official House accounts

e. Only House-approved security software and House-contracted cloud services will be used[11]

f. Electronic systems will be kept in compliance with House cybersecurity standards, including backup and software update policies

g. All electronic data-at-rest (i.e., stored) will be encrypted (this includes desktop and laptop computers, tablets, smartphones, and authorized removable media)

---

[9] For example, the House-approved Correspondence Management Systems (CMS), which may be utilized for tracking whistleblower matters, typically include functionality for restricting access to only specific staff; consult your vendor for further assistance. Offices using a shared file system (e.g., OneDrive) can consult with their tech support partner for guidance on implementing need-to-know access restrictions.

[10] House Information Security Policy 2.0, Protecting Information and Information Systems from Unauthorized Use (Oct. 3, 2023), generally prohibits USB storage devices on House desktops and laptops; limited exemptions are allowed.

[11] See the list on HouseNet, https://housenet.house.gov/page/Cloud.

h. Removable media will be labeled appropriately

i. Hard-copy information will be labeled appropriately and stored securely

j. Electronic communications and files containing House sensitive information will be encrypted prior to transmission on any public access system, such as e-mail or via the internet. Consider:

   i. The encryption features of Microsoft Outlook when communicating with other House staff (encryption is not on by default)

   ii. The encryption features of Microsoft Teams, OneDrive, and SharePoint when collaborating with other House staff (encryption features are enabled by default)

   iii. The encryption features of Office365 Message Encryption when communicating with a non-House account

   iv. The password protect feature in applications, such as Word or Acrobat, before attaching that file to an email when communicating with a non-House account (share that password via some other channel)[12]

   v. Your House-contracted Box account, when sharing with a non-House account (see Authorized Cloud Services for details)

   vi. The Signal app, for end-to-end encryption of messages and attachments (see Authorized Cloud Services for details)

      - House authorization is contingent on setting messages to expire within one week. To ensure continuity of operations, arrange to preserve relevant messages before they expire (e.g., screenshot, copy, download)

   vii. Whistleblower Intake or Tipline webforms that provide end-to-end encryption[13]

k. Hard-copy information and removable media in transit will be labeled, securely wrapped, and shipped with a tracking number

l. Individual House policies and procedures will be followed to return electronic media containing House sensitive information when no longer needed or when leaving employment with the House

m. Printed documents containing House sensitive information will be shredded when no longer needed in accordance with House records requirements[14]

12. Third party sharing.

The general prohibition, under the House Code of Official Conduct, on public disclosure of the identity of, or personally identifiable information about, a whistleblower will guide any third-party sharing of sensitive whistleblower information: *Information will not be shared*

[12] Note that the email metadata is unencrypted.

[13] See Whistleblower Communications Tools, https://housenet.house.gov/page/5436.

[14] Consult the Office of Art and Archive, a division of the Office of the Clerk, for records management advice and assistance with identifying records for permanent retention; see https://housenet.house.gov/page/3919.

outside the Office without the prior, written consent of the whistleblower.[15] However, limited exceptions will be made for the purpose of confidential consultations with House support offices, such as Office of General Counsel, the Committee on Ethics, and the Office of the Whistleblower Ombuds.

a. The Office may (notwithstanding the exceptions in Clause 21 of the House Code of Official Conduct) share sensitive whistleblower information outside of the Office under the following conditions:[16]

   i. Prior to any third-party sharing, the terms of the third party's future use of the information, including further sharing and public release, will be negotiated. The whistleblower will be invited to participate in this negotiation or specify in advance any requested boundaries around the use of their information

   ii. On a case-by-case basis, identifying information and metadata will be stripped out or masked before sharing. The whistleblower will be invited to inspect what is to be shared to help ensure the adequacy of this process

   iii. Sensitive information will be encrypted when transmitted on any public access system, such as e-mail or via the internet[17]

13. House resources for additional support.

a. Office of the Whistleblower Ombuds, https://whistleblower.house.gov

b. House General Counsel, https://housenet.house.gov/page/4035

c. House Office of Cybersecurity, https://housenet.house.gov/page/4400

d. CAO Technology Partners, https://housenet.house.gov/Interact/Pages/Section/ContentListing. aspx?subsection=4365

e. Office of Art and Archives, https://housenet.house.gov/page/3919

[15] Sensitive information shall not be shared with Artificial Intelligence (AI) tools (e.g., ChatGPT), unless explicitly approved; See House Information Technology (HITPOL) 08.00, Artificial Intelligence (Aug. 8, 2024).

[16] This may also entail sharing a whistleblower's identity with a federal agency to obtain the release of records pertaining to the whistleblower (after execution of a Privacy Act and HIPAA release). In cases where the whistleblower has requested confidentiality, the use of a privacy release to obtain documents from the agency increases the likelihood that the whistleblower's identity will be revealed. In those cases, alternative channels for obtaining the information should be identified and used. Consult the Office of the Whistleblower Ombuds for further guidance.

[17] See the specific guidance for encrypting sensitive communications in paragraph 11, above.