Smithsonian Institution

SMITHSONIAN DIRECTIVE 118,

September 15, 2020

PRIVACY POLICY

1. PURPOSE

This directive establishes the Smithsonian Institution (SI) roles and responsibilities associated with individual privacy interests, and sets forth policies and procedures for the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of personally identifiable information (PII) and sensitive PII (sPII), which are defined below. This directive also articulates the Smithsonian Privacy Principles which serve as the foundation for the Smithsonian's Privacy Program.

2. BACKGROUND

As a trust instrumentality of the United States, the Smithsonian Institution is not subject to many of the laws that govern information privacy for Executive Branch agencies.[1] However, the Institution applies information privacy best practices to support its activities as a 501(c)(3) organization whose mission is "to increase and diffuse knowledge" and adopts the specific Privacy Principles set forth in Section 5, below, as the foundation for its privacy policies and procedures.

3. APPLICABILITY/SCOPE

This directive applies to all Smithsonian employees and Affiliated Persons (as defined in Section 4) and records containing PII or having privacy implications.

---

[1] Such laws include the Privacy Act, the E-Government Act of 2002 (Pub. L. No. 107–347), the Federal Information Security Management Act (FISMA), and numerous Office of Management and Budget (OMB) guidance documents (M-16-24, M-10-23, M-10-22, M-17-12, and Circular A-130).

This directive does not apply to collection objects, library and archival materials, their digital surrogates, or their supporting documentation (e.g., registrarial records) that contain PII/sPII. Those materials shall be created, collected, used, processed, stored, maintained, disseminated, disclosed, and disposed of in accordance with SD 600, Collections Management, and each unit's specific collection and archival policies. However, if sPII is discovered in a collection, the unit must contact the Privacy Office for guidance to ensure the information is protected. However, business or financial records (e.g., vendor enrollment forms) containing PII/sPII about individuals associated with a collection item (i.e., artists, donors, collectors, or researchers) are considered PII/sPII and are subject to this directive.

This directive addresses personal privacy interests only. It does not address other attributes of data that may warrant a higher level of care in its handling or disclosure. Several other Smithsonian Directives designate certain types of Smithsonian information or data as sensitive or confidential. (See Section 8, "References.") As discussed in those directives, or as may be required by applicable law, information or data that falls within this designation may require a higher level of care in its handling and treatment.

4. DEFINITIONS

Affiliated Persons. For the purposes of this directive, the term Affiliated Persons is defined as: (i) contractors who access SI networks, facilities, or perform work similar to Smithsonian employees, such as employees of temporary help firms; (ii) volunteers, as defined in SD 208, Standards of Conduct Regarding Smithsonian Volunteers; (iii) interns and Fellows; (iv) emeriti, as defined in SD 206, Emeritus Designations; (v) visiting researchers, including scientists, scholars, and students; (vi) research associates, as defined in SD 205, Research Associates; (vii) Friends of the National Zoo (FONZ) employees, Smithsonian Early Enrichment Center (SEEC) employees, and employees of federal/state/local agencies who access SI networks or facilities; and (viii) Regents and Advisory Board members.

Breach. A breach is defined in SD 119, Privacy Breach Policy as the *suspected or confirmed* compromise, loss of control, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose.

Children's Online Privacy Protection Act (COPPA). COPPA refers to a statute enforced by the Federal Trade Commission regarding the protection of children's personal information when they engage in online activities. For purposes of COPPA, children are defined as individuals under 13 years old. In accordance with SD 950, Management of the Smithsonian Web, the Smithsonian, although not subject to COPPA, follows it as a best practice, as reflected in the Smithsonian Kids Online Privacy (SKOP) Statement.

Fair Information Practice Principles (FIPPs). FIPPs are widely accepted principles that should be applied when evaluating information systems, processes, programs, and activities that affect personal privacy. While there have been many iterations since their origin in the 1973 federal Government report from the Department of Health, Education, and Welfare Advisory Committee, *Records, Computers and the Rights of Citizens*, the core principles remain unchanged. For the purposes of this policy, the Smithsonian observes the FIPPs as set forth in Section 5 below.

Members of the Public. For the purposes of this directive, the term Members of the Public refers to individuals who are neither Smithsonian employees or Affiliated Persons, but still have interactions with the Institution. Common examples include, but are not limited to, customers at Smithsonian stores (online and in person), museum visitors, and participants in educational programs and summer camps.

Personally Identifiable Information (PII)[2]. Information about living individuals which may or may not be publicly available, that can be used to distinguish or indicate an individual's identity, and any other information that is linked or linkable to a living individual, such as medical, educational, financial, or employment information. Examples of PII include, but are not limited to:

- General Personal Data: full name, maiden name, alias, full date of birth;
- Address Information: street address or email address;
- Security Information: password, security question responses (e.g., mother's maiden name); and
- Personal Characteristics: photograph or other audio or visual material that identifies an individual's fingerprint, handwriting, voice signature, or facial geometry.

Please note that sensitive PII (sPII) is a subset of PII. See below for definition.

Privacy Assessment (PA). A PA refers to an online form Units are required to complete as part of the Privacy Review and Approval Process, which is described in Section 6, "Policy."[3] A PA is required for all systems (paper, electronic, or other media) which create, collect, use, process, store, maintain, disseminate, disclose, and dispose of the Smithsonian's PII/sPII.

Privacy Program Handbook. The *Privacy Program Handbook* sets forth supporting Privacy Program procedures, sample forms, and updated versions of the Institution's public-facing Privacy Statement. The Smithsonian Privacy Officer (SPO) shall review the *Privacy Program*

---

[2] Physical copies of publications containing or labeled with PII or professional business cards are an exception to the definition of PII.

[3] Prior to fiscal year (FY) 2020, the Smithsonian leveraged non-automated tools (i.e., the Privacy Threshold Analysis (PTA) and the Smithsonian Privacy Impact Analysis (SPIA), privacy risk assessment tools) to conduct privacy reviews. Effective in October of 2017, all new IT System privacy reviews and approvals are completed using an automated tool. In August of 2019, the automated tool was expanded to also include non-IT System privacy reviews (i.e., paper).

Handbook annually and update the document, if necessary, to reflect evolving changes in privacy and information technology that affect privacy.

Privacy Review and Approval Process. The Privacy Review and Approval Process refers to the process used by the Smithsonian Privacy Office to review and approve all Unit projects, programs, or initiatives that seek to create, collect, use, process, store, maintain, disseminate, disclose, and dispose of PII/sPII or projects with privacy implications. The Privacy Review and Approval Process is more thoroughly described in Section 6, "Policy," in the subsection on Privacy Reviews and Approvals.

Sensitive Personally Identifiable Information (sPII). A subset of PII that, if disclosed or used, could lead to harm to the individual (i.e., identity theft with the intention to do financial harm). Examples of sPII include but are not limited to:

- Social Security Number (SSN) or personal Tax Identification Number;
- Driver's license or Government-issued identification number;
- Credit card number with or without an access code;
- Bank account number with or without a personal identification number or password;
- Medical information (i.e., a diagnosis or condition); and
- Biometric identifiers (e.g., iris scans, retina scans, fingerprints).

Smithsonian Kids Online Privacy (SKOP) Statement. The SKOP Statement refers to the Smithsonian Privacy Statement regarding its policy and practices for collecting and protecting personal information from children under the age of 13. The SKOP Statement and associated Frequently Asked Questions (FAQs) and procedures are modeled after COPPA, and are further described in Section 6, "Policy," below, in the subsection on PII Collected from Minors, and in the *Privacy Program Handbook*.

Smithsonian Units (Units): Collectively refers to all Smithsonian museums, research centers, and offices.

5. SMITHSONIAN PRIVACY PRINCIPLES

The Smithsonian adopts the following nine principles, modeled after the FIPPs,[4] as the foundation of its Privacy Program. These privacy principles (hereinafter referred to as the Smithsonian Privacy Principles) shall be considered whenever Smithsonian projects, programs, or initiatives create, collect, use, process, store, maintain, disseminate, disclose, and dispose of PII/sPII, regardless of the medium.

1. **Access and Amendment**. The Smithsonian shall provide individuals with appropriate access to their PII and appropriate opportunity to correct or amend their PII.

[4] These FIPPs are modeled after those principles included in OMB *Circular No. A-130, Managing Information as a Strategic Resource*, Appendix II, p. 2.

2. **Accountability**. The Smithsonian shall be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. The Smithsonian shall also clearly define the roles and responsibilities with respect to PII for all employees and Affiliated Persons and provide appropriate training to all employees and Affiliated Persons who have access to PII.
3. **Authority**. The Smithsonian shall only create, collect, use, process, store, maintain, disseminate, disclose, and dispose of PII if it has the authority to do so, and should identify this authority in the appropriate notice.
4. **Minimization**. The Smithsonian shall only create, collect, use, process, store, maintain, disseminate, disclose, and dispose of PII that is directly relevant and necessary to accomplish a legitimate business purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.
5. **Quality and Integrity**. The Smithsonian shall create, collect, use, process, store, maintain, disseminate, disclose, and dispose of PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.
6. **Individual Participation**. The Smithsonian shall involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII. The Smithsonian shall also establish procedures to receive and address individuals' privacy-related inquiries.
7. **Purpose Specification and Use Limitation**. The Smithsonian shall provide notice of the specific purpose for which PII is collected and should only create, collect, use, process, store, maintain, disseminate, disclose, and dispose of PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.
8. **Security**. The Smithsonian shall establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal.
9. **Transparency**. The Smithsonian shall be transparent about information policies and practices with respect to PII, and provide clear and accessible notice regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII.

6. POLICY

As a trust instrumentality of the United States whose mission is "the increase and diffusion of knowledge," the Smithsonian shall create, collect, use, process, store, maintain, disseminate, disclose, and dispose of PII/sPII in a manner that does not adversely impact the integrity of, or the public's confidence in, the Smithsonian, its work, or its mission. Smithsonian

employees and Affiliated Persons shall exercise care when handling PII/sPII. All Smithsonian Privacy Principles and the terms of this directive shall apply whether collection of PII/sPII is internal (e.g., collected from and about Smithsonian employees and Affiliated Persons) or external (e.g., collected from and about members of the public, such as visitors, customers, and donors), or whether the collection occurs by the Unit or through a Smithsonian-contracted third party who is acting on the Unit's behalf to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of the PII/sPII.

The Smithsonian Privacy Program

The Smithsonian Privacy Program is administered by the Smithsonian Privacy Office, located within the Office of the Chief Information Officer (OCIO), and led by the Smithsonian Privacy Officer (SPO). The SPO is responsible for developing, implementing, and maintaining a Smithsonian-wide privacy program designed to ensure compliance with all applicable statutes, regulations, and policies regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by Smithsonian employees and Affiliated Persons. The SPO is also responsible for developing and evaluating privacy policy, managing privacy risks at the Institution, and ensuring the delivery of privacy training to all Smithsonian staff and Affiliated Persons who handle PII as a routine part of their job responsibilities.

Data Governance at the Smithsonian

Collection, Use, Access, Storage, and Dissemination of PII

Smithsonian employees and Affiliated Persons shall exercise an appropriate degree of care when creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of PII to maintain its integrity, and prevent unauthorized access with the potential for misuse. Access to PII shall be restricted to those Smithsonian employees, Affiliated Persons, and, if applicable, third parties who have a valid business "need to know." PII shall be protected by administrative, technological, and physical means commensurate to its sensitivity level and risk of harm to the individual if the PII were to be compromised.

In accordance with the Smithsonian Privacy Principles, Smithsonian employees and Affiliated Persons shall collect only PII that is necessary, and limit its use to the specific purpose intended for which it is collected, for the duration of the particular project, program, or initiative and for any necessary archiving of the PII. When collecting PII from individuals, whether by electronic or physical (i.e., paper) means, employees and Affiliated Persons shall take care to ensure that the purpose of the collection is clearly stated and the individual is

voluntarily providing consent, whether explicitly or implicitly[5], to the collection, use, and, if applicable, sharing or posting of the PII.

Authorized and Need-to-Know Access to PII and sPII

Employees and Affiliated Persons shall only be permitted to access or use PII maintained by the Smithsonian when it is in furtherance of their official duties and solely for authorized purposes. Similarly, even where an employee or Affiliated Person has the authorized ability to access PII or sPII as part of his/her duties (such as an authorized user in an information technology [IT] system), the employee or Affiliated Person shall still only access that information on those occasions when he/she has a valid business reason to know it. Employees and Affiliated Persons may also be permitted to handle or use PII on a project, IT system or website basis, for the purpose and duration of that project. The Unit shall determine those employees and Affiliated Persons and the level to which they shall be permitted to access and use PII for the project, program, or initiative.

All employees and Affiliated Persons who handle or use sPII must be authorized to do so. Employees and Affiliated Persons may be authorized by the nature of their official duties, such as the Office of Human Resources (OHR) when handling personnel documents containing employee Social Security Numbers, or the Office of Finance and Accounting (OF&A) when handling tax identification numbers or bank account information in setting up and maintaining vendor accounts. In both instances, these employees and Affiliated Persons have specific access rights in the respective IT systems that create, collect, use, process, store, maintain, disseminate, disclose, and dispose of this information. Employees and Affiliated Persons may also be authorized by their supervisor or Unit director (depending on the nature of the project) to handle or use sPII on a project, IT system or website-basis, or as specified by contract, for the purpose and duration of that project, program, or initiative.

Employees and Affiliated Persons shall handle other employees' and Affiliated Persons' PII/sPII in accordance with the terms of the applicable directives. Employees and Affiliated Persons shall properly secure and not disclose any other personnel information that by applicable law or Smithsonian policy or procedure is deemed to be confidential or is considered sensitive data[6].

---

[5] An example of "implicit" consent could involve a member of the public contacting the Smithsonian via email with an inquiry. This action gives the Smithsonian implicit consent to use the person's email address to respond to the inquiry. However, the individual is not consenting to any secondary uses of the PII by the Smithsonian.

[6] SD 807, Requests for Smithsonian Institution Information, sets forth categories of Smithsonian information that are exempted from a disclosure request. The Collections- and Archives-related SDs 600, 501, 502, and 609 also reiterate that information about collections objects may be shared only when proper permission or consent has been obtained.

Disclosure of PII

Unless authorized to do so by consent of the provider or owner of the PII, contract, Smithsonian policy, or applicable law, employees and Affiliated Persons shall not disclose or permit the unauthorized access, maintenance, and/or dissemination of PII/sPII[7]. Disclosure of such information without consent could violate an individual's privacy rights and expose the individual to risk of harm such as identity theft.

Disciplinary Action

Staff and Affiliated Persons must take care to comply with the general principles and specific provisions of this policy. If any doubt exists as to whether an activity or planned activity would violate these standards, employees/Affiliated Persons are obligated to seek advice immediately from the SPO. Failure to comply with these standards is cause for remedial or disciplinary action in the case of employees, or disqualification, modification, or separation of the affiliation in the case of Affiliated Persons.

PII Collected from Populations with Special Considerations

Employees and Affiliated Persons

Smithsonian employees and Affiliated Persons shall have no expectation of privacy in the Smithsonian's use of their business information, which includes their name, job title, grade, salary, duty station or business address, position description, business telephone number, and business online contact information.[8] Thus, their business contact information (the scope of which can be found in the Active Directory profile) is not considered PII when used independent of other personal information.

As stated in SD 931, Use of Computers, Telecommunications Devices, and Networks, Smithsonian employees and Affiliated Persons shall also have no expectation of privacy while using Smithsonian-provided computers, telecommunications devices, and networks; or in any email, World Wide Web logs and data, text message, voice mail, or other files or data created, transmitted, or received while using Smithsonian computers, devices, or networks.

The Smithsonian shall have the right to monitor employees' and Affiliated Persons' use of and access to these records in order to ensure continuation of business or to investigate possible misconduct, privacy, or security incidents. In addition, to preserve the integrity and security of its technological systems and personal property assets, authorized employees may use location-based technologies such as geo-locational services or devices to find Smithsonian-provided devices, systems, databases, and tools.

---

7 Please contact the Privacy Officer before disclosing sPII concerning a deceased individual.
8 5 *Code of Federal Regulations* (CFR) 293.311 — Availability of Information lists information about present and former federal employees that is available to the public.

Minors

The Smithsonian is committed to protecting the privacy of minors. Minors are a critical audience for many of the Smithsonian's educational and outreach programs but are part of a protected class that may not have an appropriate understanding of the importance of personal or private information. Therefore, Units shall work with the SPO to minimize the collection of personally identifiable or personal information from minors, regardless of age, where or how it is collected, and safeguard any information collected.

The collection of personal information from children under 13 years old via websites and online services is inherently sensitive. The Smithsonian maintains a SKOP Statement that articulates its policy and practices for collecting personal information from children under 13. Units shall work with the SPO to ensure that all child-directed Smithsonian websites, online services, mobile applications, and on-site interactive activities that communicate over the Web comply with, and include a link to, the SKOP Statement. Refer to the *Privacy Program Handbook f*or the SKOP Statement and SKOP procedures.

Non-U.S. Citizens

Prior to collecting and/or using personally identifiable information from or about non-U.S. citizens, Smithsonian employees and Affiliated Persons must contact the Smithsonian Privacy Officer for specific guidance and initiate the requisite Privacy Review and Approval Process described below.

PII Collected by Third Parties on Behalf of the Smithsonian

Any third party contracted by the Smithsonian to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII/sPII on the Institution's behalf and for the Institution's subsequent use shall be required to maintain the PII/ sPII's confidentiality, integrity, and availability in accordance with this directive, as well as other applicable Smithsonian policies and procedures, including SI-147B, *Smithsonian Institution Privacy and Security Clause*.

The SPO shall work with other SI Units, including the Office of Contracting and Personal Property Management (OCon&PPM), the Office of Sponsored Projects (OSP), and the Office of General Counsel (OGC), to ensure the applicable privacy-related terms and conditions are included in contracts and agreements (e.g., SI-147B, *Smithsonian Institution Privacy and Security Clause*) that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII/sPII by the third-party contractor for the Unit's use. In addition, at the time of the collection, Units shall be required to provide or post an appropriate SPO-approved notice (i.e., online or on paper) to the identified individuals that the third party collected the PII/sPII on the Unit's behalf.

Compliance

Privacy Reviews and Approvals

Units must obtain the SPO's approval as part of the privacy review process prior to creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, or disposing of any PII/sPII. The review may be initiated through the Technical Review Board process, outlined in SD 920, IT Life Cycle Management, if it meets the threshold of a new technology at SI.

Units shall be responsible for undergoing a privacy review on any (i) new project, program, or initiative, or (ii) existing project, program, or initiative where the implementation of a change would impact how PII/sPII is created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of. Units shall also contact the Privacy Office for an updated privacy review on a previously approved project in the event of a proposed material change, or after a period of three years, whichever comes first. If it is determined during the privacy review that PII/sPII will be created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of, in paper or electronic form, a Privacy Assessment (PA) must be completed. Reviews that determine no PII/sPII will be collected do not require a PA. However, there may be instances when the SPO determines that, although no PII/sPII will be collected, significant privacy implications still exist. In this case, the SPO may require the completion of a PA to document how privacy risk(s) will be mitigated. *(Please refer to the* Privacy Program Handbook *chapter on "Privacy Review and Approval Process" for additional information and guidance on completing a PA.)*

In the case of sPII, which presents a high risk of harm to individuals if it were to be compromised, the Unit will be required to demonstrate the following as part of the Privacy Review and Approval Process:

- a bona-fide need to collect the sPII that justifies the associated risk;
- its ability to implement and sustain higher standards of care and protection for the sPII, such as, but not limited to, minimization of the number of employees and Affiliated Persons authorized to have a "need to know" to access the sPII;
- its plan to keep the sPII confidential; and
- its ability to implement protections against unauthorized movement or dissemination of the sPII.

Smithsonian data containing PII/sPII cannot be used in a test environment. During the Privacy Review and Approval Process, the SPO will work with the Unit to ensure that methods for handling PII/sPII are implemented. Units shall contact the SPO or refer to the

Privacy Program Handbook chapter on "Guidance for Handling PII and sPII" for supporting procedures.

Similarly, for any PII/sPII created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of by a technological information system, website, or Web application, the Unit shall also work with the Office of the Chief Information Officer (OCIO) IT Security office to ensure that appropriate technological security controls, protections, and procedures are implemented in accordance with SD 920, IT Life Cycle Management, SD 931, Use of Computers, Telecommunications Devices and Networks, and SD 950, Management of the Smithsonian Web. A Unit's collection of credit card or payment card information shall also be subject to additional Payment Card Industry Data Security Standards (PCI-DSS) as discussed in SD 309, Merchant Accounts, Payment Cards, and the PCI Data Security Standard.

In addition, the SPO may direct the Unit to coordinate with other administrative units to ensure compliance with other applicable Smithsonian policies and procedures.[9]

Privacy Statements/Notices

In accordance with SD 950, Management of the Smithsonian Web, the SPO maintains standard *Smithsonian Privacy Statements* which reflect the principles of the Institution's overall Privacy Program and are posted at www.si.edu/privacy and www.smithsonianmag.com/about/privacy/.

The SPO may also create customized privacy notices for a particular website or Web application, which more directly describe the particular website's collection and use of PII, such as those posted on child-directed websites and Web applications in accordance with the SKOP Statement. All privacy notices shall incorporate the Smithsonian Privacy Principles and policy in this directive.

Units shall place a link to the standard, applicable Privacy Statement or a customized notice on all Smithsonian internal and external facing websites and Web applications (including those operated on behalf of the Smithsonian).

The SPO shall update all Privacy Statements and notices appropriately to reflect changes in the Privacy Program, associated procedures, or as required by applicable law.

[9] Such policies and procedures include, but are not limited to, OSP regarding SD 606, Research Involving Human Subjects; Office of Public Affairs regarding SD 814, Management of Official Smithsonian Social Media Accounts; and OCIO regarding SD 950, Management of the Smithsonian Web, and SD 931.

Privacy Statements and notices must also be available in both machine- and human-readable formats. See SD 950, Management of the Smithsonian Web, and refer to the *Privacy Program Handbook* for the current versions of the standard Smithsonian Privacy Statements and the SKOP Statement.

PII Inventory

The Privacy Officer is responsible for conducting inventories of the Smithsonian's PII holdings every three to five years.[10] In between updates, new and revised PAs will be leveraged to make incremental updates to the Inventory. Any systems identified during subsequent inventories as requiring a requisite privacy review will follow the standard review process outlined above and in SD 118, *Privacy Program Handbook*.

Compliance Testing

The Smithsonian Privacy Officer shall periodically test Units' compliance with Smithsonian privacy requirements to safeguard PII in physical form.[11] The results of these tests shall be used to develop and implement strategies to mitigate risks and augment Privacy Program guidance/training on the proper handling of PII/sPII in physical form.

Retention and Disposition of Records Containing PII/sPII

Certain records containing PII/sPII may have to be retained for a specified period of time to fulfill requirements set by law or applicable Smithsonian policy. When it is necessary to retain sPII, it shall be secured against unauthorized disclosure. However, all Smithsonian records containing PII/sPII shall be retained for only as long as the applicable purpose exists. To reduce risk, the holding of sPII for "historical" purposes is discouraged.

When applicable, appropriate retention and disposition of records containing PII or sPII should be addressed in any contracts with third-party vendors. Units shall comply with the Smithsonian Libraries and Archives (SLA) applicable records retention schedule as well as their own Unit-specific records retention policies.

Paper records containing sPII shall be disposed of using a method that will prevent recovery or use (e.g., crosscut shredding). sPII shall be removed from removable media, external drives, and portable media, in accordance with OCIO Technical Note Media Protection Policy and Procedures, IT-930-TN26.

---

[10] The Privacy Officer led the Smithsonian's baseline comprehensive inventory of PII holdings in 2018 (in paper and electronic formats). The results of the inventory were included in the *PII Inventory Final Report in support of closing Inventory related Findings from the Fiscal Year 2015 Audit Report of the Smithsonian Institution's Privacy Program (August 31, 2018).*

[11] The Smithsonian initiated this form of compliance testing on September 28, 2017.

Training and Awareness

All employees and Affiliated Persons who are provided access to Smithsonian network accounts are required to complete annual Computer Security Awareness Training, which currently includes general information for handling and safeguarding Smithsonian data, including PII/sPII. Employees and Affiliated Persons who handle PII as a regular part of their job responsibilities are required to complete role-based privacy training. The SPO shall develop, update, and deliver additional privacy training and awareness programs to Units that use PII/sPII. Such training may be held in order to address compliance with this policy and/or to support security measures necessary to maintain the privacy of Smithsonian data.

The SPO shall coordinate with Units as needed to provide privacy guidance on internal and external procedures and policies. This may include, but is not limited to, SI-wide Announcements, awareness campaigns, targeted training, compliance tests, standard operating procedures, and rules of behavior.

Privacy Breach Reporting

As set forth in SD 119, Privacy Breach Policy, Smithsonian employees and Affiliated Persons are required to report a privacy breach or the suspicion of a privacy breach to the OCIO Service Desk, Office of Protection Services (OPS), or the SPO. Refer to SD 119, Privacy Breach Policy, and the SD 119 Appendix, Privacy Breach Reporting and Notification Process, for further guidance.

7. RESPONSIBILITIES

The Smithsonian Privacy Officer (SPO) is responsible for developing privacy policies and procedures to support the Smithsonian Privacy Program, and monitoring compliance with these policies and procedures. The SPO provides general advice on privacy matters, coordinates with OGC and OCon&PPM to provide subject-matter expertise on privacy issues, and oversees the provision of privacy training to Smithsonian employees and Affiliated Persons.

As Chair of the Privacy Council,[12] the SPO convenes the Council and coordinates the Smithsonian's response in the event of a confirmed privacy breach. The SPO is responsible for notifying the Office of Inspector General in cases of a confirmed significant privacy breach.

The SPO is also responsible for reporting significant privacy issues, including proposed changes to this directive, to the Under Secretary for Administration on a semi-annual or as-needed basis.

[12] In accordance with SD 119, Privacy Breach Policy, in the event of a confirmed privacy breach, the SPO convenes the Privacy Council and serves as the Privacy Council Chair.

The Smithsonian Privacy Office is responsible for conducting privacy reviews of Smithsonian projects, programs, and initiatives that create, collect, use, process, store, maintain, disseminate, disclose, and dispose of PII/sPII and, where appropriate, will coordinate with other Smithsonian Units (e.g., OPS, OCon&PPM, OF&A, OSP, OHR, and OGC) to confirm that appropriate administrative, technical, and physical controls are in place for Smithsonian projects, programs, and initiatives that handle PII/sPII. The SPO also works collaboratively with the Director of Information Technology Security to ensure the computer security awareness training (CSAT) includes up-to-date privacy content.

The Office of the Chief Information Officer (OCIO) is responsible for conducting security reviews, and ensuring sufficient security controls are in place and maintained to protect all information technology systems, including websites and applications that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII/sPII. OCIO monitors computer networks and systems, implements the appropriate technological response to a privacy incident or breach, and resolves any identified security deficiency which permitted the compromise or breach to occur. OCIO advises the Units on how to technologically secure PII/sPII, as well as its other sensitive and confidential information. In accordance with SD 950, Management of the Smithsonian Web, OCIO ensures that all public-facing Smithsonian branded and operated websites include a functioning link to the current version of the applicable Smithsonian Privacy Statement and that the Statement is accurately translated in machine-readable format.

The Office of Protection Services (OPS) is responsible for monitoring the physical security of Smithsonian facilities, systems, records, and property. OPS conducts background investigations of, and prepares Smithsonian credentials for, all employees and Affiliated Persons who will have physical access to facilities or systems. In the event of a privacy breach, OPS investigates and corrects any physical security defects that may have permitted or allowed unauthorized access.

Smithsonian Institution Libraries and Archives (SLA) is responsible for conducting a program of records management services for Smithsonian Units, advising on the disposition of records and pertinent documentary materials, and operating a Records Center for the temporary storage of scheduled records.

The Office of Contracting and Personal Property Management (OCon&PPM) is responsible for developing and implementing policies and procedures for the control and proper record keeping of all Smithsonian personal property, including items used to create, collect, use, process, store, maintain, disseminate, disclose, and dispose of PII/sPII. OCon&PPM is also responsible for developing, implementing, and overseeing policies and procedures concerning the acquisition, contracting or licensing of goods or services that may create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII/sPII (e.g., contracts and agreements for websites, or applications [apps]). OCon&PPM coordinates with the SPO and the Director of Information Technology Security on updates to SI 147B, *Smithsonian Institution Privacy and Security Clause*.

The Office of Human Resources (OHR) is responsible for providing policy guidance and assistance to Smithsonian employees concerning employment and personnel matters. OHR maintains the Institution's official personnel records and works with the Units on procedures to handle employee and personnel information and documentation which routinely contain employee PII/sPII.

The Office of the Inspector General (OIG) has the authority to investigate events leading up to a privacy breach, and may work with OPS on legal and/or criminal issues involved in the investigation, such as the issuance of a subpoena to recover stolen property.

Smithsonian Units, Employees, and Affiliated Persons are responsible for complying with this directive and with the Smithsonian Privacy Principles whenever their Smithsonian projects, programs, and initiatives involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of PII/sPII. To the extent that employees and Affiliated Persons, in the performance of their official duties, may have or be granted access to PII/sPII, their access shall not exceed their authorized need to know. Units with Smithsonian records containing PII/sPII shall generally follow applicable record retention schedules maintained by SLA as well as their own internal policies.

Smithsonian Directors are responsible for taking actions intended to ensure that their employees and Affiliated Persons comply with this directive.

8. REFERENCES

SD 103, Smithsonian Institution Standards of Conduct

SD 107, Office of the Inspector General

SD 118, *Privacy Program Handbook*

SD 119, Privacy Breach Policy

SD 119 Appendix, Privacy Breach Reporting and Notification Process

SD 124, Protection of Minors Policy

SD 205, Smithsonian Institution Research Associates

SD 206, Emeritus Designations

SD 208, Standards of Conduct Regarding Smithsonian Volunteers

SD 212, *Federal Personnel Handbook*, Chapter 731

SD 213, *Trust Personnel Handbook*, Chapter 731

SD 214, Equal Employment Opportunity Program

SD 222, Smithsonian Health and Wellness Services

SD 224, Identity Management Program

SD 309, Merchant Accounts, Payment Cards, and the PCI Data Security Standard

SD 314, Contracting

SD 315, Personal Property Management Manual (Appendix A)

SD 503, Management of Archives and Special Collections in the Smithsonian Institution

SD 600, Collections Management Policy

SD 603, Exhibition and Program Planning

SD 606, Research Involving Human Subjects

SD 609, Digital Asset Access and Use

SD 709, Smithsonian Institution Internships

SD 807, Requests for Smithsonian Institution Information

SD 809, Philanthropic Financial Support

SD 814, Management of Official Smithsonian Social Media Accounts

SD 920, IT Life Cycle Management

SD 931, Use of Computers, Telecommunications Devices, and Networks

SD 950, Management of the Smithsonian Web

SI 147B, Smithsonian Institution Privacy and Security Clause

Smithsonian Memo, “Designation of the Smithsonian’s Senior Agency Official for Privacy,” November 14, 2016

Smithsonian Memo, “New Targeted, Role-based Privacy Training,” October 13, 2016

Federal Guidance

OMB Circular A-130, Managing Information as Strategic Resource

OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information

---

SUPERSEDES:	SD 118, March 11, 2014.
INQUIRIES:	Office of the Chief Information Officer
	(OCIO) — Privacy Office: 202-633-5129.
RETENTION:	Indefinite. Subject to review for currency 36 months from date of issue.
