Smithsonian Institution

SMITHSONIAN DIRECTIVE 118,
March 11, 2014

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 collection, use, storage, and dissemination of personally identifiable information (PII) and sensitive personally identifiable information (sPII), which are terms defined below. This directive also applies the Smithsonian Privacy Principles which serve as the foundation for the Smithsonian's Privacy Program.

2. BACKGROUND

The Smithsonian Institution respects privacy and is committed to protecting the personal privacy of its visitors, employees, volunteers, interns, Fellows, scholars, research associates, donors, and contractors. As a trust instrumentality of the United States, the Smithsonian frequently collects, maintains, and disseminates PII to carry out its mission to increase and diffuse knowledge. The Smithsonian is committed to properly handling and protecting PII.

However, designating a data element as PII does not in and of itself determine how the data should be properly handled and protected. How PII is used or collected in different contexts, or combined with other PII data, can change its sensitivity level and the risk of harm to individuals if their PII were to be compromised. For example, an individual's first and last name when coupled with an address or telephone number presents a relatively low risk of harm, but when coupled with a Social Security number or credit card number, presents a high risk of harm. In order to ascertain the sensitivity level of PII and the risk of harm to an individual if the PII were

2. BACKGROUND (continued)

to be compromised, the Smithsonian must evaluate the totality of the circumstances surrounding its use of the PII, such as the context, purpose, aggregation with other PII elements or other information, and the location in which it will be used, collected, stored, or disseminated.

Although the Smithsonian Institution is not subject to many of the laws that govern information privacy for Executive Branch agencies,[1] it 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 Generally Accepted Privacy Principles (GAPP) as the foundation for its privacy policies and procedures.

This SD 118, *Privacy Policy*, replaces the previous SD 118, *Privacy Breach Notification Policy*. The *Privacy Breach Notification Policy* is now renumbered to SD 119.

3. APPLICABILITY/SCOPE

This directive applies to all Smithsonian Staff and Affiliated Persons, as they are defined below.

This directive does not apply to collection objects, archival materials, their digital surrogates, or their supporting documentation that contain PII or sPII. Those materials shall be collected, used, and protected in accordance with SD 600, *Collections Management*, and each Unit's specific collection and archival policies.[2]

This directive addresses personal privacy interests only, and 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

---

[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) Memorandums (M-05-08, M-07-16, M-06-19, M-06-15, M-08-21, and M-99-18).

[2] Refer to SD 600, *Collections Management*; SD 501, *Archives and Records of the Smithsonian Institution*; SD 503, *Management of Archives and Special Collections in the Smithsonian Institution*; and SD 609, *Digital Asset Access and Use*. PII and sPII, in this context, may only be used, disclosed, or made publically available to diffuse knowledge, where the collecting or archival unit has obtained appropriate permission or consent from the appropriate owner or lender.

3. APPLICABILITY/SCOPE (continued)

or confidential.[3] 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]

Any violation of this policy may be subject to disciplinary action or other appropriate actions.

4. DEFINITIONS

Affiliated Persons. For purposes of this directive, the term Affiliated Persons is defined as the following: (i) contractors who perform work similar to Smithsonian employees, such as employees of temporary help firms; (ii) volunteers, as defined in SD 208, *Ethical Standards for SI 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*; and (vii) Regents and Advisory Board members.

Children's Online Privacy Protection Act (COPPA). COPPA refers to a statute administered by the Federal Trade Commission Act 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.

Generally Accepted Privacy Principles (GAPP). GAPP refers to 10 generally accepted privacy principles developed by privacy professionals in North America as a framework for effective organizational privacy programs.

Personally Identifiable Information (PII). Personally identifiable information (PII) refers to information about individuals which may or may not be publically available, that can be used to

---

[3] Examples of sensitive data include protected species and cultural/Native American Repatriation data (SDs 600, 603, and 503); human subject research data (SD 606); SI employee/personnel data (e.g., in SDs 212, 213, 214, and 222); investigative information (e.g., SDs 224 by the Office of Protection Services [OPS] and107 by the Office of Inspector General [OIG]); contract data prior to award, contractor/vendor labor rates/pricing (e.g., SDs 314 by the Office of Contracting and Personal Property Management [OCon&PPM]); and donor information (e.g., SD 809).

[4] Refer to SD 920, *Life Cycle Management*, which enumerates a list of sensitive data elements, and SD 807, *Requests for Smithsonian Institution Information*, which restricts the disclosure of certain types of Smithsonian information consistent with exemptions set forth in the Freedom of Information Act.

4. DEFINITIONS (continued)

distinguish or indicate an individual's identity, and any other information that is linked or linkable to an 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;
- Personal Identification Number: Social Security number, passport number, driver's license number, taxpayer identification number, financial account number, credit card number;
- Security Information: password, mother's maiden name; and
- Personal Characteristics: photographs and voice files that identify individuals, fingerprints, handwriting, biometric data such as retina scans, voice signatures, and facial geometry.

Privacy Breach. A privacy breach is defined in SD 119, *Privacy Breach Notification Policy* (at the time of this writing), as the unauthorized acquisition, access, use, or disclosure of PII or sPII that compromises the security or privacy of such information. A breach includes the compromise of a Smithsonian information system that could allow unauthorized access to PII or sPII. A breach also includes the loss or theft of any physical property (including papers) that could have the same result.

Privacy Program Handbook. The *Privacy Program Handbook* sets forth supporting Privacy Program procedures, sample forms, and updated versions of the Institution's privacy policy statement. The Smithsonian Privacy Officer (SPO) shall review and update the *Privacy Program Handbook* 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 SPO to review and approve all Unit projects that seek to collect, use, store, or disseminate PII or sPII. The Privacy Review and Approval Process is more thoroughly described in the subsection below, Privacy Reviews and Approvals.

Privacy Threshold Analysis (PTA). PTA refers to a form Units are required to complete as part of the Privacy Review Process, which is described below. A PTA is required for all technology or digital projects such as websites, information technology (IT) systems or mobile applications which collect, use, store, or disseminate PII or sPII.

4. DEFINITIONS (continued)

Sensitive Personally Identifiable Information (sPII). sPII is a subset of PII and is defined as certain PII data elements that, if disclosed or used in combination with other data, could lead to harm to the individual (i.e., identity theft with the intention to do financial harm). sPII generally falls into the following categories:

Category 1: sPII is the first and last name or last name and first initial in combination with one or more of the following data elements:

- Social Security number or personal Tax Identification Number;
- Driver's license or Government-issued ID number;
- Credit card number with or without an access code;
- Bank account number with or without a personal identification number (PIN) or password; or
- Medical information (i.e., a diagnosis or condition).

Category 2: Physical personally identifiable information, such as biometric identifiers: iris scans, retina scans, fingerprints, voice prints, are stand-alone data elements which are considered sensitive because of the possibility of increased risk to individuals if the information were to be compromised.

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

Smithsonian Privacy Impact Analysis (SPIA). SPIA refers to a form Units are required to complete as part of the Privacy Review and Approval Process described below. An SPIA is required as a second step after a PTA for all technology or digital projects such as websites, IT systems or mobile applications which collect, use, store, or disseminate sPII.

Smithsonian Staff or Staff. Smithsonian Staff or Staff are defined as all Smithsonian employees.

Smithsonian Units or Units. Units collectively refer to all Smithsonian museums, research centers, and offices.

5. SMITHSONIAN PRIVACY PRINCIPLES

The Smithsonian adopts the following 10 principles, modeled after GAPP, as the foundation of its privacy practices. Smithsonian Privacy Principles shall be considered whenever Smithsonian programs or initiatives involve the collection, maintenance, storage, and dissemination of PII and sPII, particularly data received from the public and via the World Wide Web.

1. **Management.** The Smithsonian shall document, communicate and assign accountability for its privacy policies and procedures.

2. **Notice.** The Smithsonian shall provide notice about its privacy policies and procedures and identify the purposes for which personal information is collected, used, retained and disclosed.

3. **Choice and consent.** The Smithsonian shall describe choices available to the individual and obtain implicit or explicit consent with respect to the collection, use and disclosure of PII and sPII.

4. **Collection.** The Smithsonian shall collect PII and sPII only for the purposes identified in the notice.

5. **Use, retention and disposal.** The Smithsonian shall limit the use of PII and sPII to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The Smithsonian shall retain PII and sPII for only as long as necessary to fulfill the stated purposes or as required by law or regulation, and thereafter appropriately dispose of such information.

6. **Access.** Where feasible, the Smithsonian shall provide individuals with access to their PII and sPII for review and update.

7. **Disclosure to third parties.** The Smithsonian shall disclose PII and sPII to third parties only for the purposes identified in the notice or with the implicit or explicit consent of the individual. In addition, although the Smithsonian is not subject to the Privacy Act, Freedom of Information Act, or the Ethics in Government Act, the Institution responds to requests for information in a manner consistent with the Acts and applicable Smithsonian Directives. Personal privacy is exempt from public disclosure under the Smithsonian's public records request policy, SD 807, *Requests for Smithsonian Institution Information*.

8. **Security for privacy.** The Smithsonian shall take reasonable steps to protect PII and sPII against unauthorized access (both physical and technological).

5. SMITHSONIAN PRIVACY PRINCIPLES (continued)

9. **Quality.** The Smithsonian shall maintain accurate, complete and relevant PII and sPII only for the purposes identified in the notice.

10. **Monitoring and enforcement.** The Smithsonian shall monitor compliance with its privacy policies and procedures, and shall maintain procedures to address privacy-related complaints and disputes.

6. POLICY

As a trust instrumentality of the United States whose mission is "the increase and diffusion of knowledge," the Smithsonian shall collect, use, store, and disseminate PII and 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 Staff and Affiliated Persons shall exercise care when handling PII and sPII. Whether collection of PII and sPII is internal (e.g., collected from and about Smithsonian Staff and Affiliated Persons) or external (e.g., collected from and about its 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 collect, use, store, or disseminate the PII and sPII, all Smithsonian Privacy Principles and the terms of this directive shall apply.

Collection, Use, Storage, and Dissemination of PII

Smithsonian Staff and Affiliated Persons shall exercise an appropriate degree of care when collecting, using, storing, or disseminating PII to maintain its integrity, and prevent unauthorized access with the potential for misuse. Access to PII shall be restricted to those Smithsonian Staff, Affiliated Persons, and, if applicable, third parties who have a "need to know." PII shall be protected by technological and/or 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 Staff and Affiliated Persons shall collect only PII that is necessary, and shall limit its use to the specific purpose intended when collected and for the duration of the particular project or effort and any necessary archiving of it. When collecting PII from individuals, whether by electronic or physical (i.e., paper) means, Staff and Affiliated Persons shall ensure that the purpose of the collection is clearly stated and the individual is voluntarily providing consent, whether explicitly or implicitly, to the collection, use, and, if applicable, sharing or posting of the PII.

6. POLICY (continued)

Prior to a Unit's collection, use, storage, or dissemination of PII or sPII as part of a new project or initiative, or an existing project or initiative implementing a material change that will result in the new collection, use, storage, or dissemination of PII and sPII, the Unit shall be required to obtain prior approval by the SPO, as described in the Privacy Reviews and Approvals subsection below. 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 Staff and Affiliated Persons authorized to have a "need to know" and access the sPII;
- its plan to keep the sPII confidential; and
- its ability to implement protections against unauthorized movement or dissemination of sPII.

For any sPII that will be collected, used, stored, or disseminated by a technological information system, website, or Web application, the Unit's privacy review and approval process shall also require prior approval by the Chief Information Officer (CIO).

During the privacy review and approval process, as defined below, the SPO will work with the Unit to ensure that methods for handling PII and 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 PII and sPII collected, used, stored, or disseminated by a technological information system, website, or Web application, the Unit shall also work with the Office of the Chief Information Officer (OCIO) to ensure that appropriate technological security controls, protections, and procedures are implemented in accordance with SD 920, *Life Cycle Management*, and 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*.

6. POLICY (continued)

PII Collected from 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 minors are part of a protected class that may not have an appropriate understanding of the importance of personal 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 collected, and safeguard any information collected.

The collection of personal information from children under 13 years old via the World Wide Web 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 are compliant with, and include a link to, the *SKOP* statement. Refer to the *Privacy Program Handbook* for the *SKOP* statement and *SKOP* procedures.

PII Collected by Third Parties on Behalf of the Smithsonian.

Any third party contracted by the Smithsonian to collect, use, store, or disseminate PII or sPII on the Institution's behalf and for the Institution's subsequent use shall be required to maintain the PII or sPII's confidentiality, integrity, and availability in accordance with this directive, as well as other applicable Smithsonian policies and procedures. Units should confirm with the SPO on whether or not the contracting of a third party to provide a service will be subject to this SD. There may be instances where a third party is hired by the Unit to provide a service that does not require the third party to collect, store or use PII or sPII on behalf of the Unit and for the Unit's use, but the third party may still do so as part of its normal business practices. If the Unit does not receive or have access to that PII or sPII, the SPO may determine that the terms of this SD do not apply.

The SPO shall work with the Units, including OCon&PPM, the Office of Sponsored Projects (OSP), and the Office of General Counsel (OGC), to ensure that applicable privacy-related terms and conditions are included in contracts and agreements that involve the collection, use, storage, or dissemination of PII or 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 appropriate SPO-approved notice (i.e., online or on paper) to individuals of the third party's collection of the PII or sPII on the Unit's behalf.

6. POLICY (continued)

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

Staff 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 a Staff member 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 IT system), Staff and Affiliated Persons shall still only access that information on those occasions when he/she has a legitimate need to know it. Staff 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 Staff and Affiliated Persons and the level to which they shall be permitted to access and use PII for the project or initiative.

All Staff and Affiliated Persons who handle or use sPII must be authorized to do so. Staff 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 (OFA) when handling tax identification, Social Security numbers, or bank account information in setting up and maintaining vendor accounts. In both instances, these Staff and Affiliated Persons have specific access rights in the respective IT systems that collect, use, store, and disseminate this information. Staff and Affiliated Persons may also be authorized by the supervisor, Unit head, or 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.

Privacy Reviews and Approvals

Units shall be responsible for undergoing a privacy review on (i) all new Smithsonian systems, processes, programs, and projects that collect, maintain, and/or disseminate PII and sPII[5] and (ii) any existing Smithsonian system, process, program or project that, with a material change, now seeks to include the collection, use, storage, and/or dissemination of PII and sPII. Similarly, Units shall be responsible for undergoing an updated privacy review on a previously SPO-approved project in the event of a proposed material change.

As part of the privacy review and approval process, the SPO shall determine whether and to what extent the project is collecting, using, storing, or disseminating PII; whether, given the

[5] Technological or digital projects may include new IT systems, websites, online services, and mobile applications (apps). Non-technical projects may include new paper surveys, comment cards, permission slips, and donor cards.

6. POLICY (continued)

totality of the circumstances and context, the collection or use presents a low, moderate, or high risk of harm (i.e., identity theft) to an individual in the event of a compromise or breach; and the further steps necessary to ensure the PII or sPII's secure handling will be done in accordance with Smithsonian privacy principles, this policy, the *Privacy Program Handbook*, and other applicable Smithsonian policies.

In addition, the SPO may direct the Unit to coordinate with other administrative units to ensure compliance with other applicable Smithsonian policies and procedures.[6] The Unit must obtain the SPO's approval as part of the privacy review process prior to collecting, using, storing, and/or disseminating any PII or sPII; and prior to entering into any third-party contracts that result in the collection, use, storage, and/or dissemination of PII or sPII.

For technology or digital projects such as websites, IT systems or mobile applications proposing to collect, use, store, or disseminate PII or sPII, the Unit shall complete a Privacy Threshold Analysis (PTA) to document and maintain an inventory of the Unit's (or its third party's) online collection or use of PII or sPII. In addition to the information above, the PTA will be used to determine whether the expected online collection or use and technological security protections complies with applicable privacy and security policies and procedures.[7] If the SPO determines that the website or online system seeks to collect, use, store, and/or disseminate sPII, the SPO will work with the Unit to prepare a Smithsonian Privacy Impact Analysis (SPIA) to document the additional measures to be implemented for the sPII. PTAs and SPIAs shall be maintained and used by the Smithsonian for internal purposes only. Refer to the *Privacy Program Handbook* chapter on "Privacy Review and Approval Process" for additional information and sample PTA and SPIA forms.

Web Privacy Notices

Consistent with SD 950, *Management of the Smithsonian Web*, the SPO maintains a standard Smithsonian privacy notice or policy statement which reflects the principles of the Institution's overall Privacy Program, and is posted at www.si.edu/privacy. The SPO may create a customized privacy notice for a particular website or Web application, such as the privacy policy

---

[6] Such policies and procedures include, but are not limited to, OSP regarding SD 606, *Research Involving Human Subjects*; OGC regarding SD 814, *Social Media Policy*; and OCIO regarding SD 950, *Management of the Smithsonian Web*, and SD 931.

[7] The PTA is also a part of the first step in the life-cycle management process for IT projects, per SD 920, *Life Cycle Management*.

6. POLICY (continued)

statement linked on the Smithsonian Enterprises (SE) websites, and the *SKOP* statement. Units shall ensure that all Smithsonian websites and Web applications (including those operated on behalf of the Smithsonian) contain a link to the standard privacy notice or customized notice. All privacy notices must also be available in both machine- and human-readable formats. See SD 950, *Management of the Smithsonian Web*.

In addition, the SPO may require a Unit to post a supplemental privacy notice within the respective website, which more directly describes 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*.

All privacy notices shall incorporate the Smithsonian Privacy Principles and policy set forth in this directive. Refer to the *Privacy Program Handbook* for the current version of the standard Privacy notice statement and the *SKOP* statement. The SPO shall update all privacy notices appropriately to reflect changes in the Privacy Program, associated procedures, or as may be required by applicable law.

Disclosure of PII

Unless specifically authorized to do so by consent of the provider or owner of the PII, contract, Smithsonian policy[8], or applicable law, Staff and Affiliated Persons shall not disclose or permit the unauthorized access, maintenance, and/or dissemination of PII and sPII. 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, and may be subject to disciplinary action.[9]

---

[8] 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 the objects may only be shared when proper permission or consent has been obtained.

[9] Staff may be subject to disciplinary action for disclosing any Smithsonian information which is of a confidential or privileged nature, per SD 103, *Smithsonian Institution Standards of Conduct*. To the extent Affiliated Persons are also subject to the requirements of SD 103 or other applicable Smithsonian Directives, they may be subject to termination of their engagement at the Smithsonian or other action for disclosing any Smithsonian information which is of a confidential or privileged nature.

6. POLICY (continued)

Retention and Disposition of Records Containing PII and sPII

Certain records containing PII or sPII may be required to be retained for a specified period of time to fulfill requirements set by law or applicable Smithsonian policy. However, all Smithsonian records containing PII or sPII shall be retained for only as long as the applicable purpose exists. Units shall comply with SD 505, *Smithsonian General Records Disposition Schedules Handbook*, maintained by Smithsonian Institution Archives (SIA) as well as their own Unit-specific records retention policies. To reduce risk, sPII held for "historical" purposes is discouraged. When it is necessary to retain sPII, it shall be secured against unauthorized disclosure.

Units shall securely dispose of paper records containing PII or sPII in accordance with applicable records disposition schedules for that Unit. 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, Disposal of Sensitive Electronic Media, IT-960-TN-15* and *930-TN-26*.

Personnel Privacy

Staff and Affiliated Persons shall handle employee and Affiliated Persons' PII and sPII in accordance with the terms of the applicable directives.[10] Staff 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 sensitive.

Smithsonian Staff 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,[11] business telephone number, and business online contact information. As stated in SD 931, *Use of Computers, Telecommunications Devices and Networks*, Smithsonian Staff and Affiliated Persons shall also

---

[10] Refer to SD 212, *Federal Personnel Handbook*; SD 213, *Trust Personnel Handbook*; SD 214, *Equal Opportunity Handbook*; SD 222, *Smithsonian Health and Wellness Services*; SD 224, *Identity Management Program*; and SD 103, *Smithsonian Institution Standards of Conduct*.

[11] 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.

6. POLICY (continued)

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

Privacy Breach

As set forth in SD 119, *Privacy Breach Notification Policy*, Smithsonian Staff and Affiliated Persons are required to report a privacy breach or the suspicion of a privacy breach to the OCIO Help Desk, OPS, or the SPO. Refer to SD 119, *Privacy Breach Notification Policy*, for further guidance.

Training and Awareness

All Staff and Affiliated Persons are required to complete annual Computer Security Awareness Training, which currently includes general information for handling and safeguarding Smithsonian data, including PII and sPII. The SPO shall develop, update and deliver additional privacy training and awareness programs to Units that use PII and sPII. Such training may be held in order to address compliance with this policy and/or, in conjunction with OCIO, to address security measures necessary to maintain the privacy of Smithsonian data.

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 to provide subject-matter expertise on privacy issues, and oversees the provision of privacy training to Smithsonian Staff and Affiliated Persons.

7. RESPONSIBILITIES (continued)

The SPO conducts privacy reviews of Smithsonian programs and initiatives that collect, use, store, and disseminate PII and sPII and, where appropriate, will coordinate with other Smithsonian Units (e.g., OCIO, OPS, OCon&PPM, OFA, OSP, OHR, and OGC) to confirm that appropriate administrative, technical, and/or physical controls are in place for Smithsonian programs and initiatives that handle PII and sPII.

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 also responsible for reporting significant privacy issues, including proposed changes to this directive, to the Under Secretary for Finance and Administration/Chief Financial Officer, Under Secretary for History, Art, and Culture, Under Secretary for Science, and Assistant Secretary for Education and Access, on a semi-annual or as-needed basis.

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 collect, use, store, and disseminate PII and 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 and 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 applicable privacy notice 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 badging credentials for, all Staff and Affiliated Persons who will have physical access to facilities or systems. In the event of a privacy incident or breach, OPS investigates and corrects any physical security defects that may have permitted or allowed unauthorized access.

Smithsonian Institution Archives (SIA) 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

---

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

7. RESPONSIBILITIES (continued)

scheduled records. Smithsonian records containing PII and sPII shall generally follow applicable record retention schedules maintained by SIA.

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 collect, maintain, and disseminate PII and 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 collect, use, maintain, secure, and disseminate PII and sPII (e.g., contracts and agreements for websites, or applications [apps]).

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

The Office of the Inspector General (OIG) is notified by the SPO of a confirmed privacy breach, and 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, Staff and Affiliated Persons are responsible for complying with this directive and with the Smithsonian Privacy Principles whenever their Smithsonian initiatives involve the collection, use, storage, and dissemination of PII or sPII. To the extent that Staff and Affiliated Persons, in the performance of their official duties, may have or be granted access to PII or sPII, their access shall not exceed their authorized need to know.

Smithsonian Directors are responsible for ensuring that their Staff and Affiliated Persons comply with this directive.

8. REFERENCES

SD 103, *Smithsonian Institution Standards of Conduct*

SD 107, *Office of the Inspector General*

SD 119, *Privacy Breach Notification Policy*

SD 205, *Research Associates*

8. REFERENCES (continued)

SD 206, *Emeritus Designations*

SD 208, *Ethical Standard for Smithsonian Volunteers*

SD 212, *Federal Personnel Handbook*

SD 213, *Trust Personnel Handbook*

SD 214, *Equal Opportunity Handbook*

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 501, *Archives and Records of the Smithsonian Institution*

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

SD 505, *Smithsonian General Records Disposition Schedules Handbook*

SD 600, *Collections Management*

SD 603, *Exhibition Planning*

SD 606, *Research involving Human Subjects*

SD 609, *Digital Asset Access and Use*

SD 807, *Requests for Smithsonian Institution Information*

SD 809, *Philanthropic Financial Support*

SD 814, *Social Media Policy*

SD 920, *Life Cycle Management*

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

SD 950, *Management of the Smithsonian Web*

CANCELLATION:	None.
INQUIRIES:	Office of the Under Secretary for Finance and Administration/Chief Financial Officer (OUSF&A/CFO) — Privacy Office: 202-633-5241.
RETENTION:	Indefinite. Subject to review for currency 24 months from date of issue.