Office of the Chief Information Officer (OCIO)
Smithsonian Privacy Office (PO)

Privacy Program Handbook

Dated: September 15, 2020

Table of Contents

1. Privacy Office Contact Information

For all questions pertaining to the Smithsonian Institution Privacy Policy, please contact the Smithsonian Privacy Officer (SPO):

Danèe Gaines Adams, SPO
Privacy Officer
Office of the Chief Information Officer
1000 Jefferson Avenue, SW
MRC 041, P.O. BOX 37012
Washington, DC 20013-7012

Phone: 202-633-5129
Fax: 202-633-0179
Email:SmithsonianPrivacyOffice@si.edu or GainesAdamsD@si.edu

2. Reporting a Privacy Breach or Suspicion of a Privacy Breach

Do you need to report a privacy breach or the suspicion of a privacy breach?

Yes, SI Employees and Affiliated Persons shall report all breaches, security incidents, and information spillage immediately, but no later than one hour after discovery, to the Office of the Chief Information Officer (OCIO) Service Deskand/or Office of Protection Services (OPS) by:

- calling the **OCIO Service Desk at 202-633-4000** (VoIP x34000) to report a privacy breach involving a Smithsonian Institution (SI) Information Technology system; or
- calling the **OPS at 202-633-9598 (VoIP x39598)** to report a privacy breach involving physical security or if OCIO is not otherwise available.

Do not report privacy breaches, security incidents, or information spillage via voice mail or email alone. Both the OCIO and OPS numbers provided are available 24 hours a day.

If in doubt, individuals should err in favor of reporting. The Smithsonian does not retaliate against individuals for good-faith reporting regardless of whether the report is substantiated. The OCIO and OPS shall immediately relay all breaches to the Privacy Council Chair who, as appropriate, will convene the Privacy Council. The Privacy Council shall assess the reports provided by the Chair and provide feedback in a timely manner. Members of the Privacy Council shall also notify the Chair of policy or procedural deficiencies they identify that could prevent or mitigate breaches.

For more information, refer to SD 119, *Privacy Breach Policy* and SD 119, *Appendix.*

3. Smithsonian Privacy Statements

A. Privacy Statement. Effective January 10, 2020 as posted at http://www.si.edu/Privacy

B. Smithsonian Privacy Statement for Philanthropic and Revenue-Generating Activities. Effective as of January 10, 2020, as posted at: https://www.smithsonianmag.com/about/privacy/

C. SKOP Statement. Effective June 18, 2014 (last declared current May XX, 2020) as posted at https://www.si.edu/privacy/kids

4. Smithsonian Kids Online Privacy (SKOP) Statement

A. The current SKOP Statement is as follows:

Smithsonian Kids Online Privacy Statement

Effective: March 11, 2014

We at the Smithsonian are committed to protecting the privacy of our visitors under the age of 13 years old ("Children" or "Child"). This Smithsonian Kids Online Privacy Statement provides an overview of what information we may collect through our websites, online services, mobile applications, and onsite interactive activities that are geared toward Children (collectively "Kid Site(s)") and what we may do with the information.

1. Generally Speaking, What Personal Information Might the Kid Sites Collect from Children, and How Is It Used?

Each of the Kid Sites is designed differently, depending on its educational purpose; consequently, the information collected from Children on each Kid Site, and the way in which the information is used, varies. Each Kid Site's "Usage Terms," "Rules," or "FAQs" will provide specific information about the collection of personal information for that particular Kid Site. Generally speaking, our Kids Sites follow these practices:

- We strive to structure our Kids Sites to be enjoyed by visitors of all ages, without having to provide personal information (i.e., as an anonymous user).
- We do not ask Children for more personal information than is necessary for participation in an activity.
- We give parents and legal guardians an opportunity to request changes to or deletion of personal information we have collected from their Children.
- Once the activity and purpose for collecting the information from the Child has concluded, we delete the information.
- If a Child sends a one-time inquiry or request, we will respond to the Child and delete the child's personal information after we answer the question or fulfill the request.
- If a Child wishes to send an email or postcard through a Kids Site, the only personal information we will ask for is the recipient's e-mail address to send the email or postcard.
- If a Child signs up for a Kids Site e-newsletter, email updates, or activity that requires multiple email contacts with a Child, we will ask the Child for his or her email address as well as the parent or legal guardian's e-mail address so we can provide notice and give the parent or legal guardian an opportunity to decline further communications from the Smithsonian to the Child.
- If a Kids Site offers an activity or game that only requires the Child to provide a user name and parent or legal guardian's email address, we will use the parent or legal guardian's e-mail address to provide notice to the parent or legal guardian of the child's interest in the activity and give the parent or legal guardian an opportunity to decline the child's participation and/or request the deletion of the parent's email address from our records.
- If a Kids Site offers an activity or game that requires the Child to provide more personal information than a user name and parent or legal guardian's e-mail address for the Child to participate in the activity (i.e. to set up a Child user account), or if the activity allows the Child to share additional information (i.e., comment on an article or blog), we will initially ask the Child for a user name and parent or legal guardian's email address in order to contact the parent or legal guardian. We will notify the parent or legal guardian about the Child's request to participate in the Kids Site, explain what information we need and why, and ask the parent or legal guardian to provide verifiable permission before the Child may participate.

2. What Information Do Our Kids Sites Automatically Collect?

We automatically gather and store the following information about site visitors so we can monitor site usage, traffic trends, functionality, and make technological improvements. This information is aggregated and stored. It will only be used for the Smithsonian's internal purposes, and will not be used to contact any Child or visitor. In particular, we automatically collect:

- The IP address used to access the Kids Site;

- The name of the domain used to access the Internet (for example, aol.com, if the visitor is connecting from an America Online

account);
- The type of browser and operating system used to access the Kids Site;
- The date and time the Kids Site was accessed;
- The pages, files, documents and links visited; and
- The domain of the website which referred the Kid to this Website (the last website the kid visited before visiting this one), if any.

3. How Do We Use Cookies on Our Kid Sites?

In addition to information collected automatically, we use cookies to support the internal functionality of the Kids Site. Cookies in this context are small pieces of data sent from the Kids Site to a visitor's browser, and stored in the browser while visiting the Kids Site. The cookies are not used to identify visitors over time or across websites. The information collected from the cookies is only used in the aggregate track site usage patterns, traffic trends, and visitor behavior. Content adjustments and visitor service improvements are made based on the data derived from cookies. Cookies may be disabled by setting your browser to refuse cookies from a Kids Site, however once disabled, certain interactive elements on the Kids Site may not function properly.

4. How Do We Keep Personal Information Secure?

We take reasonable steps to design and manage our Kids Sites technology to ensure that our information technology systems, applications and information technology infrastructure are secured. As appropriate and feasible, the Smithsonian monitors network traffic to identify unauthorized attempts to access, upload, or change information, or otherwise cause damage. Unauthorized access may be punishable by law, including criminal penalties. In addition to limiting access to Children's information to those who have a valid business "need to know," the Smithsonian requires its service provides who help maintain or operate the Kids Sites to contractually agree to protect the confidentiality, integrity, availability and security of personal information collected from Children.

5. How Can Parents or Legal Guardians Review and Request Changes to or Deletion of Their Children's Personal Information?

To the extent feasible, we allow parents or legal guardians to review personal information collected about their Children, request changes to or deletion of the information, or refuse to allow further collection or use of the information. To make any of these requests, a parent or legal guardian must contact the Smithsonian as instructed in the "Usage Terms," "Rules," or "FAQ" section of the particular Kids Site that collected the information. Such requests will be subject to the Smithsonian verifying, to its satisfaction, that the requestor is in fact the Child's parent or legal guardian.

6. When Do We Share or Disclose a Child's Personal Information?

We may share personal information collected from a Child with our service providers who have a valid business "need to know" the information and have agreed to maintain its confidentiality, integrity, availability, and security. We also may be required to disclose personal information we obtained from a Child to: (1) protect the safety of a Child; (2) protect the security or integrity of the Smithsonian Websites and services; (3) respond to judicial process and take precautions against liability; (4) the Department of Justice or in certain legal proceedings when the Smithsonian, an employee of the Smithsonian, or the United States is a party to litigation or has an interest in the litigation and the use of such records is deemed relevant and necessary to the litigation; (5) a Committee of Congress in response to a formal request; and (6) any other person or entity as the Smithsonian believes is required by law. Any further sharing or disclosure requires parental permission.

7. How Do We Use Embedded Plug-Ins, Widgets, and Links?

Within the Kids Sites there may be embedded applications, plug-ins, widgets, or links to non-Smithsonian websites (collectively "sites"). These sites operate independently and each may have its own privacy policy. When a Child visits these sites, the Child leaves the Smithsonian website and is no longer subject to Smithsonian privacy and security policies. The Smithsonian is not responsible for the privacy or security practices or the content of other sites, and placement of such sites within Kids Sites, is not intended to be an endorsement of those sites or their content.

8. How Will You Know if We Change Our Privacy Statement?

From time to time we may update this Smithsonian Kids Online Privacy Statement. When this happens, we will notify our visitors of the new provisions by publicly posting them here. If the change is material, we will send notice to the parents and legal guardians whose email addresses we have on file.

9. Who Can You Contact with Questions?

For questions, contact us:

By mail:
Smithsonian Institution
Privacy Office
P.O. Box 37012, MRC 041,
Washington, DC 20013-7012
By email: SmithsonianPrivacyOffice@si.edu
By phone: 202-633-5129

Thanks for reading this Smithsonian Kids Online Privacy Statement. We hope you have a Seriously Amazing experience when visiting our websites!

B. SKOP FAQs for Units

FAQ: Websites and Apps for Children Under 13 Years Old

Dated: November 28, 2018

On July 1, 2013, changes to the Children's Online Privacy Protection Act of 1998 (COPPA) went into effect. In accordance with SD 950, *Management of the Smithsonian Web* and *SD 118, Privacy Policy*, the Smithsonian follows COPPA as a best practice. The changes expanded the definition of what is considered to be personal information collected from a child under the age of 13, and also updated appropriate steps for providing notice to parents and obtaining prior parental consent for those collections.

What Is COPPA?

COPPA is the **Children's Online Privacy Protection Act of 1998** which governs the online collection, use, or dissemination of personal information from children under the age of 13. Per SD 950, although we are not subject to COPPA, we continue to follow it as a best practice. The Smithsonian's Privacy Statement located on all of our publically facing websites now contains a link to Smithsonian Kids Online Privacy (SKOP) Statement that affirmatively states our commitment and general practices for collecting, and protecting personal information collected from children under the age of 13.

Who Is Affected?

All Smithsonian Units that manage websites, activities on websites, mobile applications, online services or computer interactive applications that connects to the internet or a wide-area network within an exhibition, that are directed to children under the age of 13 (collectively "Kid Site(s)").

What Is Personal Information Collected from a Child under 13?

For online activities only, personal information from a Child under 13 is any of the following:

a. First and last name
b. A home or physical address, including just the street name and city or town
c. Online contact information (e.g., email address, IM user identity, video chat identifier,

VOIP identifier)

d. A screen or user name that functions as online contact information (where it functions in the same manner as online contact information (e.g., permitting direct contact with the child user online)
e. Telephone Number
f. Social Security Number
g. A photograph, video, or audio file, where such file contains the Child's image or voice;
h. A Persistent Identifier that can be used to recognize a user over time and across different websites or online services (e.g., a device identifier, cookie identifier, serial number, IP address) unless they support the internal operations of the website/activity, are not used to contact the child directly, and will not be shared with an unaffiliated third party.[1]
i. Geo-locational information precise or sufficient enough to identify a street name and name of a city or town. [2]
j. Information concerning a Child or the parents of that Child that the Smithsonian collects online from the Child and combines with an identifier above.

When Will I Have to Obtain Parental or Legal Guardian Consent?

Unless the activity falls within a limited exception to COPPA, consent will be required for those Kid Sites where the Unit wants to obtain, use, or share (make publically available) personal information from a child under 13. Generally speaking, if a Kid Site requires users under the age of 13 to have their own user accounts, then the Unit will have to obtain parental or legal guardian consent.

How Will Parental or Legal Guardian Consent Work?

The method of obtaining consent will vary depending on the Unit's activity and how the Unit intends to use the personal information once obtained. Generally speaking, where a Kid Site seeks to obtain personal information from the Child, the Kid Site will need to request a parent email address from the Child. The email address is then immediately used to contact the parent or legal guardian, convey the Child's interest in the Kid Site, and provide information about the personal information requested, including how it will be used, and how the parent or legal guardian can provide consent to the Smithsonian prior to the Child's participation in the Kid Site. In some limited cases, the Unit may be able to have the parent or legal guardian consent as a click through agreement in the same email. In most other cases, the parent or legal guardian will have to print, sign, and submit back to the Smithsonian an attached consent form.

What Are the Exceptions Where Consent Is Not Required?

There are limited instances where a Unit can collect minimal personal information from a Child under 13, without having to obtain parental or legal guardian consent. A Unit's Kid Site can collect minimal personal information from a Child under 13 if the Kid Site is set up in a way that it can either treat all of its users as anonymous users and/or immediately delete any of the minimal personal information obtained. Units may also collect an email address to respond to a child's one-time inquiry, question, or request (such as an Ask the Expert activity), but then must immediately delete the information.

Additionally, if a Unit would like to be able to send program updates or newsletters or other ongoing communications to a Child, it may collect only a user name and parent email address to provide a parent or legal guardian with notice of the child's interest in an activity and the information to have them opt out of these communications. In this case, only notice to the parent or legal guardian is required.

[1] This can be included in metadata that is a part of the upload of user content (e.g., metadata in a photo with or without people in the photo). Some persistent identifiers may be acceptable to support a website's internal operations and provided the information is not disclosed.
[2] Metadata in photos may include this information. Also, zip codes alone are not considered Personal Information.

Can Teachers Provide Consent on Behalf of Parents or Legal Guardians?

No, teachers are not considered to be legal guardians of children and can't sign parental consent forms. However, there may be limited instances where a teacher or school has implemented a parental consent program such that the Smithsonian can rely on it for purposes of verifying consent for the Unit's project. In most cases, however, the Unit will need to have a parent teacher consent form created for the project. Units should work with the SPO and OGC on parental consents.

Are There Additional Requirements for a Kids Site?

Yes, there are additional requirements for Kid Sites. A Kid Site will need to link to the Smithsonian Kids Online Privacy Statement; post a SPO-generated project specific privacy notice regarding the personal information being collected, used, stored, and/or shared; provide direct notice to parents and legal guardians prior to collecting a Child's personal information; and unless approved by the SPO to fall within an exception, obtain verifiable parental consent from parents or legal guardians. Once the information has been collected, the Unit (and/or its contracted third party) will be required to maintain its confidentiality, availability, and integrity. In the event that parents or legal guardians request to have their children's information deleted or removed, the Unit will be required to honor the request within a reasonable period of time. [3] In all cases, Units should strive to offer a Kid Site experience that can be enjoyed as an anonymous user (without having to provide personal information).

Who Can I Talk to for More Information?

If you have additional questions or concerns or are in the process of working on a project which may involve the online collection of personal information from children under 13, please contact the Privacy Officer, Danèe Gaines Adams at GainesAdamsD@si.edu or 202-633-5129.

[3] This turnaround time will depend on the Unit's capability for being able to turn it around for the Kids Site, but somewhere between ten (10) to fourteen (14) days of receipt is recommended.

C. SKOP — Detailed Procedural Guidance.

OVERVIEW

The Smithsonian, as part of its mission to increase and diffuse knowledge, engages online with, and provides educational mobile applications, online educational programs, websites, and other activities, for visitors under the age of 18 ("Minors").[4] The Smithsonian is committed to the protection of Minors' privacy and safety and to the extent feasible and appropriate, will minimize its online collection of personally identifiable information from Minors, and design safe and secure online experiences for Minors, even as online technologies and Minors' uses of such technologies evolve.

If a Unit seeks to engage with Minors online, or otherwise collect, use, store, or disseminate "Personal Information" (as defined below) from Children, the Unit must contact the SPO for prior review and approval. The SPO will work with the Unit to ascertain the Unit's intended use of the Minor's information and whether the proper administrative (that is, contractual and technological) controls will be in place to properly secure and use the information once collected.

DEFINITIONS

(a) "Children" or "Child" means individual(s) under the age of 13.
(b) "Teens" or "Teen" means individual(s) between the ages of 13 and 17.
(c) "Parents" or "Parent" includes parents and legal guardians.
(d) "Online Activity" means a Smithsonian-branded mobile application, as well as any Smithsonian-branded or Smithsonian-operated website (or section within a website), online activity or service, or on-site computer interactive that communicates over the internet.
(e) "Kids Site or Site(s)" mean those Online Activities that are geared toward Children.
(f) "Personal Information" includes any of the following information if provided online by a Child:
- First and last name
- A home or physical address, including just the street name and city or town
- Online contact information (e.g., email address, IM user identity, video chat identifier, VOIP identifier)
- A screen or user name that functions as online contact information (where it functions in the same manner as online contact information (e.g., permitting direct contact with the child user online)
- Telephone Number
- Social Security Number
- A photograph, video, or audio file containing the Child's image or voice
- A persistent identifier that can be used to recognize a user over time and across

[4] If a Unit's collection of information is intended as a systematic investigation designed to contribute to generalized knowledge, the Unit should follow the procedures set forth in Smithsonian Directive 606 (Research Involving Human Subjects).

different websites or online services (e.g., a device identifier, cookie identifier, serial number, IP address)[5]
- Geo-locational information precise or sufficient enough to identify a street name and name of a city or town[6]
- Information concerning a Child or the parents of that Child that the Smithsonian collects online from the Child and combines with an identifier above

ONLINE ACTIVITIES FOR CHILDREN

Generally, Smithsonian Online Activities are intended for general audiences and do not permit Children to participate in interactive features.[7] Nevertheless, Smithsonian policy permits Units to interact online with Children provided that, as a best practice, the Unit complies with the Children's Online Privacy Protection Act.[8] The below procedures reflect the Smithsonian's interpretation of these best practices in the context of the Smithsonian's mission. The procedures in this section apply to Online Activities that:

- are directed to Children and involve the collection, use, or dissemination of a Child's Personal Information; or
- knowingly collect Personal Information from a Child (even if not directed toward Children).

a. Procedures.

(i) Smithsonian Kids Online Privacy Statement (SKOP).
(a) Units' Kids Sites must comply with the terms of the SKOP, a copy of which is at Appendix A above.
(b) Kids Sites shall link to the SKOP as directed by the SPO.
(c) The SKOP may be updated at anytime by the SPO. If the update is material in nature, the SPO will coordinate with Units to send notifications about the update to Parents whose email address is on file with the Units.

(ii) Units seeking to create a Kids Site or otherwise collect, use, store, or disclose Personal Information must contact the SPO in advance for guidance, including a determination of whether these procedures, or other appropriate precautions, are warranted.

(iii) If the SPO determines that the Unit's Kids Site is subject to these procedures, and unless a variation is approved by the SPO, the Unit must do all of the following:

(a) Not condition the Child's participation in the Kids Site on the collection of more Personal Information than is necessary for participation;

[5] This can be included in metadata that is a part of the upload of user content (e.g., metadata in a photo with or without people in the photo).
[6] Metadata in photos may include this information.
[7] www.si.edu/termsofuse
[8] Smithsonian Directive 950 (Management of the Smithsonian Web).

(b) In consultation with the SPO, develop a notice statement describing the collection of Personal Information for the Kids Site, its use, and possible disclosures (the "Notice") to be included as part of the Kid Site's FAQs, Rules, or Usage Terms;

(c) Provide a clear and prominent link to the Notice on the Kids Site's home page, or its equivalent, and wherever the Unit or its vendors will collect Personal Information;

(d) Deliver a copy of the Notice statement directly to a Child's Parent before collecting Personal Information from the Child, or using or disclosing it;

(e) Unless approved by the SPO to fall within an exception listed below, obtain verifiable parental consent from the Parent prior to the collection, use or disclosure of Personal Information from the Child;

(f) To the extent feasible and appropriate, if the Unit will be sharing the Personal Information with third parties, give Parents the choice as to whether the Child's information will be shared with third parties;

(g) Deliver notice of material updates to the SKOP or Notice to affected Parents;

(h) Work with OCIO to maintain the confidentiality, integrity and availability (e.g., the security) of the Personal Information collected, including Parental consents;[9]

(i) Limit the number of Employees and Affiliated Persons who will have access to Personal Information, and instruct such Employees and Affiliated Persons that Personal Information may only be shared on a valid business "need-to-know" basis;

(j) Work with OCon&PPM/OGC/OSP (as applicable) to ensure that each vendor that has a need for access to Personal Information is contractually restricted to using the information for Smithsonian purposes and obligated to protect the confidentiality, availability, and integrity of the Personal Information;

(k) Provide a method for Parents to review any Personal Information collected about their Children, request changes to the information, request deletion of the information, and refuse further collection or use of the information.[10] Units shall be responsible for verifying that the requestor is in fact the Child's Parent before complying with the request;

(l) Unless an exception below applies, the Unit shall delete all information collected from a Child within Smithsonian records within a reasonable time[11] of its receipt of the Parent's request; and

(m) Retain Personal Information for only so long as is reasonably necessary to fulfill the purpose for which the information was collected.

The SPO is available to consult on any of the above procedures.

---

[9] OCIO is available to consult with Units on developing appropriate procedures and technology to keep the Personal Information secure, including a record of all active Parental consents received, the date received, and the associated Parent contact information to be used to notify the Parent in the event the SKOP is updated by the SPO or for other occasions as may be required as set forth in the SKOP.

[10] The Office of General Counsel is available to consult with Units regarding any request for modification, deletion, or revocation of consent.

[11] Reasonable turnaround time can vary, but somewhere between ten (10) to fourteen (14) days of receipt is recommended.

b. Methods for Obtaining Verifiable Parental Consent. The Unit shall work with the SPO to determine which method of verifiable parental consent is appropriate for a particular Kids Site. The SPO will determine how rigorous or reliable the parental consent will need to be based on how the Unit desires to use the Child's Personal Information. The SPO will also determine if the Unit's use falls within one of the exceptions listed below such that verifiable parental consent is not required.

(i) Internal Use. If the Unit is collecting Personal Information for "internal use" only, the Unit may use the "email plus" method to obtain consent.

- "Internal Use" means the Personal Information is collected and will be used for internal requirements for the Kid Site, such as to sustain the internal operations necessary to maintain or analyze its functioning for the user experience, provided that the information is not shared outside the Smithsonian, unless that sharing is required to maintain the Kid Site's internal operations and the third party is contractually (i) restricted from using the information for its own purposes, and (ii) obligated to protect the confidentiality, integrity, and availability of the information.
- "Email plus" means: (i) the Unit sends Notice to the Parent's online contact address and requests the Parent to consent by return message; and (ii) if consent is received by the Unit, the Unit sends a confirming message to the Parent (via letter, email, or phone call) reminding the Parent about his or her registration for the Kid Site on behalf of his or her Child, the Notice, his or her agreement to the applicable terms and conditions, and information about whom to contact in case the creation of the account was in error. If consent is not received, the Unit may not collect Personal information from the Child.

(ii) On-site Activities. If an educational, noncommercial, online activity is included as part of a Unit's on-site exhibition or program, and the collected Personal Information will be for Internal Use only, the Unit may use a click through agreement followed by a confirmatory email. To qualify for this method:

(a) The registration process must be designed for the Parent to complete as a Parent Account, which the Child may also use;

(b) The registration presents the Notice, and other applicable terms and conditions, as a click-through agreement; and

(c) The Unit must send a confirmatory email to the Parent, reminding the Parent about his or her registration for the Online Activity, the Notice, his or her agreement to the applicable terms and conditions, and information about whom to contact in case the creation of the account was in error.

c. Public Sharing or Disclosure of the Personal Information. If the Unit intends to allow public sharing of Personal Information as part of the Kid Site (for example allowing Children to participate in social media, chat rooms, message boards, blogging, exchanging information with other users of the Kid Site, or similar activity) or to disclose Personal Information with third parties[12], the following methods are available:

[12] A Unit may share Personal Information with its vendors who are contractually (i) restricted to using the information only for support of the internal operations of the Kids Site, including technical support and order fulfillment, and (ii) obligated to maintain its security and confidentiality and will not use it for their own purposes. Units should work

a) Obtaining a signed permission form from Parents via email, postal mail or facsimile;
b) Accepting and verifying a credit card number in connection with a transaction;
c) Taking calls from Parents, through a toll-free telephone number ed by trained personnel;
d) Obtaining an email accompanied by a Parent's digital signature; or
e) Implementing an alternative SPO-approved technological solution developed or purchased for the Kids Site.

IMPORTANT: The Unit must give Parents the option to agree to the collection and use of Children's Personal Information without having to agree to the public disclosure of the information *unless* the public disclosure is the central feature of the Online Activity; that is, the Online Activity is social networking, chat rooms, message boards, and blogging.

IMPORTANT: Depending on the Unit's goals for use of Personal Information, the Parental permission form also should include copyright and liability releases. The Office of General Counsel is available for advice on appropriate release language.

IMPORTANT: Units seeking to share the results of a survey, interview, or observation of a Minor's behavior in a public setting (e.g., at a conference or professional meeting) also may be required to follow the procedures set forth in Smithsonian Directive 606 (Research Involving Human Subjects).

d. School as Intermediary. Potentially, if Children seeking to participate in a Kids Site are doing so as part of a School or other Educational Institution (collectively "School")-based program, the Unit may be able to rely on the School or teacher as an intermediary for parental consent.

IMPORTANT: Unless a variation is approved by the SPO, if the Smithsonian obtained parental consent through a School or teacher as intermediary, the Smithsonian will only use and retain the Personal Information for the duration of the then-current school year.

e. Exceptions to Obtaining Parental Consent. In certain limited instances, the Unit's Online Activity may be subject to an exception so that prior verifiable parental consent is not required or a modification or deletion of Personal Information would be inappropriate. Specifically:

- The Kids Site doesn't collect, use, or disclose any Personal Information (i.e., anonymous users);[13]

with OCon&PPM/OGC/OSP to ensure that their contracts with any vendors contain the necessary restrictions and obligations. Further, to take advantage of this option, the Unit must have clearly described its and its vendors' collection, use, storage, and disclosure practices in its Notice so that Parents can make an informed decision about their Children's participation.

[13] Units may be able to fall within this exception where the Kids Site collects information from a child and then immediately strips out all Personal Information and immediately deletes the Personal Information from all Smithsonian records.

- Collecting a Child's or Parent's email address (in the first instance) to provide direct notice and seek verifiable parental consent;
- Collecting an email address to respond to a one-time request from a Child and then the Unit deletes it (that is, to answer a one-time question);
- Collecting an email address to respond more than once to a Child's request — for example, if a Child subscribes to an e-newsletter. In this case, the Unit shall notify the parent that it is communicating regularly with the Child and give the Parent the opportunity to stop the communication before sending or delivering a second communication to a Child;
- Disclosing Personal Information collected to protect the safety of a Child, protect the security or integrity of the site, or take precautions against liability, as well as to (i) the Department of Justice or in certain legal proceedings when the Smithsonian, an employee of the Smithsonian, or the United States is a party to litigation or has an interest in the litigation and the use of such records is deemed relevant and necessary to the litigation; (ii) a committee of Congress in response to a formal request; and (5) any other person or entity as the Smithsonian believes is required by law; or
- Persistent identifiers, such as cookies, may be used (i) only to support the internal operations of the Online Activity, website or online service[14];(ii) the information is not used to contact the Child; (iii) no other personal information is collected; and (iv) is not disclosed to third parties[15].

ONLINE ACTIVITIES FOR TEENS

Units seeking to direct an Online Activity to individuals between the ages of 13 and 17 ("Teens"), or otherwise collect, use, store, or disseminate information from Teens, must contact the SPO for prior review and approval. Even though the Smithsonian may design an Online Activity for Teens, in reality, it may attract younger audiences. Accordingly, depending on the nature of the Online Activity, as well as the Unit's intentions for the collection, use, storage, or disclosure of information collected from Teens, the SPO may direct the Unit to implement privacy protections, such as:

- Screen for age. If the Unit learns that a user is a Child, block the Child's participation and delete any Personal Information submitted.

[14] Persistent identifiers employed for the sole purpose of providing support for the Unit's internal operations of the Online Activity means activities that are necessary for the Online Activity to maintain or analyze its functioning; perform network communications; authenticate users, personalize user's content, maintain user-driven preferences such as game scores or character choices in virtual worlds; serve contextual (not behavioral) advertising or cap the frequency of advertising; protect the security or integrity of the user, website, or online service; ensure legal or regulatory compliance; or fulfill a request of a child as permitted.

[15] Third parties' use of persistent identifiers on a Unit's Kids Site, may be permitted, provided: (i) the persistent identifier's sole purpose is to support the third party's internal operations, or both the Unit and the third party's internal operations; (ii) the third party will not collect more Personal Information than necessary; and (iii) the third party is contractually obligated to protect the confidentiality, availability, and integrity of Personal Information.
Units must work with OCon&PPM/OGC/OSP (as applicable) to ensure that the contract between the Smithsonian and the third party contains the appropriate restrictions and obligations.

- Include specific privacy information in the "FAQs," "Usage Terms" or "Rules" for the Teen site.
- Work with OCIO to protect the confidentiality, integrity, and availability of any Personal Information collected.

Additionally, the SPO may also encourage the Unit to incorporate a method of direct notice and/or parental consent for the Online Activity, as a best practice.

UNINTENTIONAL RECEIPT OF INFORMATION FROM CHILDREN

If a Unit operating a general audience Online Activity learns that a Child has shared Personal Information with the Smithsonian, the Unit should consult with the SPO to determine whether the Unit should delete the information, respond to the Child on a one-time basis and then delete the information, or follow the procedures set forth above for Online Activities for Children.

Guidance for Handling PII and sPII

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 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 created, collected, used, processed, stored, maintained, disseminated, disclosed, and disposed of.

A. Handling Records Containing PII

- Only accessible by Employees and Affiliated Persons with a valid business need to know the information.
- Online collection of PII is required to be encrypted using TLS 1.2 or higher and SHA-256 technology (i.e., in emails, Web forms, form fields, input boxes, etc.).
- PII may only be stored, saved or hosted on approved Smithsonian equipment. If stored on shared drives, access shall be restricted to only those individuals who also have a valid business need to know the information.
- Unless encrypted as an attachment, PII should not be shared within or outside of the Smithsonian network via email.
- Paper records containing PII shall be protected from unauthorized access, and should be locked in a drawer, file cabinet, desk, safe, or other secure place when not in use.
- Paper records containing PII shall not be left unattended, and shall be removed from view on desks or computer desk tops when Employees and Affiliated Persons step away from their workstations.
- For fax transmissions containing PII, Employees and Affiliated Persons shall ensure that the recipient is aware that the fax is en route and verify its receipt. It is recommended that faxes containing PII also be sent encrypted or through a Virtual Protocol Network.
- Employees and Affiliated Persons shall refrain from conducting discussions about PII in public areas or over internet-based conference calls or video calls.
- When the purpose for collecting the information no longer exists, records containing PII must be disposed of using a method that will prevent recovery or use (e.g., cross-cut shredding for paper records).

B. Handling Records Containing sPII

- General.
    - Only accessible by Employees and Affiliated Persons who are

authorized and who have a valid business need to know the information for the purpose.
  - Records containing sPII shall be disposed of in accordance with applicable record retention disposition schedules, and by a method that will prevent recovery or use (e.g., cross-cut shredding for paper).
  - Employees and Affiliated Persons shall refrain from conducting discussions about sPII in public areas or over internet-based conference calls or video calls.

- Paper Records.
  - To the extent possible, Employees and Affiliated Persons shall refrain from maintaining or creating physical (paper) records containing sPII. If physical copies need to be created, then where possible, sPII elements should be redacted.
  - Employees and Affiliated Persons are prohibited from printing and/or storing records containing sPII while teleworking.
  - Paper Records containing sPII shall be protected from unauthorized access, and must be physically secured when not in use and/or kept under the control of the authorized individual and when in transit to prevent unauthorized access or loss.
  - Paper Records containing sPII shall never be left unattended. When not in use, they must be stored in a locked drawer, file cabinet, desk, safe, or other secure place.
  - Employees and Affiliated Persons should limit any fax transmissions of sPII unless they can be encrypted or sent through a Virtual Protocol Network. When faxing, Employees and Affiliated Persons shall ensure that the recipient is aware the fax is en route and immediately verify receipt.

- Electronic Records.
  - Any online collection of sPII shall be encrypted using TLS 1.2 or higher and SHA-256 or better technology (in emails, Web forms, form fields, input boxes).
  - IT Systems: sPII shall only be saved, stored, or hosted on approved Smithsonian equipment. sPII shall only be stored on shared drives if access is restricted to only those individuals who have a valid business need to know the information (and when the information is protected by password or access restrictions). Smithsonian Employees and Affiliated Persons should consult unit IT staff for additional information.
  - Emails: Unless encrypted as an attachment, sPII may not be shared within or outside of the Smithsonian network via email. When requesting that sPII be sent via email, Employees and Affiliated Persons should tell recipients how to secure the information, as detailed below:

- "I am requesting that you provide sensitive personally identifiable information, which, if lost, compromised, or disclosed without authorization could result in substantial harm. To protect your privacy, please provide the information in an encrypted attachment and provide the password under separate cover (e.g., a separate email, in person, or via phone)."
- Removable/Portable Media and External Drives: sPII shall not be stored on CDs, hard drives, USB drives, DVDs, floppy disks, flash drives, memory sticks, etc., unless the device is encrypted. Good encryption shall also be used when transferring files containing SSNs. Smithsonian Employees and Affiliated Persons should consult Unit IT Employees for additional information concerning this requirement. See SD 931, Use of Computers, Telecommunications Devices, and Networks, for further information.
- Laptops, Tablets, Mobile Phones, and Other Devices: sPII shall not be stored on Smithsonian laptops unless approved encryption is used. Laptops containing sPII shall remain under the control of the person to whom the laptop is assigned to the greatest extent possible (e.g., laptops containing sPII shall not be checked as baggage at the airport). OCIO guidance prohibits the storage of sPII on non-Smithsonian and/or unencrypted laptops. See SD 931 for further information. For further information concerning encryption, contact the OCIO Service Desk at ociohelp@si.edu or 202-633-4000.

For further information concerning encryption, contact the OCIO Service Desk at ociohelp@si.edu or 202-633-4000.

- Mail: Paper records containing sPII shall be sealed in opaque envelopes or placed in courier bags when in transit (e.g., an employee physically transporting records from the Castle to Capital Gallery is directed to place records in a sealed envelope or a courier bag). Records containing sPII shall be mailed (in a sealed, opaque envelope) via the United States Postal Service (USPS) First Class Mail, Priority Mail. Employees and Affiliated Persons may also use a courier service such as FedEx or UPS that confirms receipt when mailing records containing sPII. Employees and Affiliated Persons shall not mail unencrypted CDs, DVDs, hard drives, USB drives, or other media containing sPII.

Questions about handling PII and sPII should be directed to the SPO.

5. General Privacy Program Procedures

A. Privacy Review Process

Units are responsible for contacting the Smithsonian Privacy Office for any (i) new project, program, or initiative, or (ii) existing project, program, or initiative where the implementation of a change would impact how PII is created, collected, used, processed, stored, maintained, disseminated, disclosed, and disposed of. The Privacy Office will conduct 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.

How to Initiate the Privacy Review Process

The review may be initiated through the Technical Review Board (TRB) process outlined in SD 920, IT Life Cycle Management, if it meets the threshold of a new technology at SI. The Privacy Program Specialist, or SPO, will ask questions during the Tailoring call to determine if a PA is required. Even if no PA is required, the Privacy Office may require evidence in the form of a development site, screen shots, or wire frame to validate no PII/sPII is inadvertently collected. The Tailoring Agreement will document the follow-up privacy action items. However, please note that if a system designated as "No PA Required" is later discovered to be collecting PII, or to have other undisclosed privacy implications, documentation will be modified and a PA may be needed prior to implementation.

The review may also be initiated through a direct email to SmithsonianPrivacyOffice@si.edu, a phone call to any Privacy Office, or another form of contact/outreach. If it is determined by the TRB administrator that review by the TRB is not needed, the Privacy Office will still schedule a phone call with the Unit POC to determine if a PA, or other privacy action, is required. If the answer is no, the Unit POC will receive a follow-up confirmation email documenting that no PA is needed, and outlining any next steps. This direct outreach to the Privacy Office must be completed for both paper and electronic systems. If it is determined a PA will be required, the Unit POC will be directed to next steps for initiating the PA.

There are some instances where no PII/sPII will be collected, but significant privacy implications still exist. In this case, a Unit POC may be asked to complete a PA to document how privacy risk will be mitigated.

Is a Privacy Assessment Required?

At the initial stage of the privacy review process, the Privacy Program Specialist, or Smithsonian Privacy Officer (SPO), will work with the Unit Point of Contact (POC) to determine if a Privacy Assessment (PA) is required. The following questions may be asked depending on the specifics of the system:

- Will any form of PII/sPII as defined in SD 118, Privacy Policy be collected, used, stored, or disseminated?
- Will any third-party vendors be involved in this system?
- Has the third-party service been properly procured per SI policy?
- Will PII/sPII from children/minors be collected into this system?
- Will PII/sPII from non-U.S. residents be collected into this system?

Conducting a PA

There are three types of privacy assessments at the Smithsonian:

- For PII within an IT system, website, mobile application, or online activity, complete the *Archer Privacy Assessment (PA) for IT Systems*. Contact the

Privacy Office to initiate this process. Based on the technology used, you may also be required to take the system through the Technical Review Board (TRB), which is administered by OCIO (SAPATRB@si.edu). Guidance on how to complete a PA for IT Systems can be found on the Privacy Office Prism page at http://prism2.si.edu/SIOrganization/PrivOfc/Pages/Archer_PA_Guidance.asp x

- For PII collected, used, stored, or disseminated within a paper-based system, complete the *Archer Privacy Assessment (PA) for Paper Systems*. Examples of such systems may include paper surveys, comment cards, permission slips, donation slips, or personnel files. Guidance on how to complete a PA for IT Systems can be found on the Privacy Office Prism page at http://prism2.si.edu/SIOrganization/PrivOfc/Pages/Archer_PA_Guidance.asp x
- For systems that do not collect, use, store, or disseminate PII/sPII but still have significant privacy implications, a PA may still be required.

Please note that paper/electronic hybrid systems (systems which have both paper, IT, or other mediums that make up one cohesive business process), will only require one PA to be completed in either the Paper or IT PA template. Use whichever template will host the majority of the business process. For example, a comment card system that scans paper cards for storage in an online database and then promptly disposes of the paper records, should be assessed using the IT System PA template.

Tracking the Status of Your PA

The PA review process is iterative. Once the template is filled out and submitted to the Privacy Office, your reviewer may have follow-up questions or additional requirements as the specifics of the system come into view. The status of your PA will be documented in the Monthly Aging Report that goes out to all Unit POCs and Unit Directors/Designees with a PA "in process" with the Privacy Office. Additionally, if you are listed as the "submitter" on the PA, you will receive automated updates through Archer when the status of your review changes.

If at any point the Unit becomes aware that the project/initiative will be cancelled or postponed, it is imperative to let the Privacy Office know as soon as possible so a notation can be made in that month's Aging Report.

There are five possible statuses for a Smithsonian PA:

- With OCIO IT Security to Configure the Archer Package — All Archer PAs for IT Systems must be tied to a package in Archer. Additionally, if a user is new to the Archer System, he or she must be granted access by the IT Security Team. Once the package has been created, or access has been granted, the Unit POC will receive a link to the PA via email so he or she can begin to fill-out the template.
- With the Privacy Office for Review (Initial and Final Review) — The Privacy Office representative assigned to your project conducts the initial review. The SPO, or his/her designee, conducts the final review and grants approval. If the timeline has shifted or there are any changes to the system since the Unit POC filled out the template, please email SmithsonianPrivacyOffice@si.edu for guidance. Be aware that adequate time should be built into the project plan to allow for the review between submission to the Privacy Office and final approval.
- With the Unit for Action — The PA has either never been submitted to the Privacy Office (the template is still with the Unit), or the PA was returned to the Unit with comments/action items. While it is understood that addressing these comments/action items may take some time, any project that has been with a Unit for more than a year without action will be administratively withdrawn via email.

- Approved — For PAs (both Paper and IT), the Archer system will generate an email notifying you that the final approval has been granted by the Privacy Office. Ensure you work to address any other outstanding action items (such as TRB, Human Subjects Research, IT Security Review, or Accessibility) before going live with the initiative/project. Remember, per SD 118, Privacy Policy, you must reach back out to the Privacy Office for an updated review if there is a material change, or after a period of three years, whichever comes first.
- Withdrawn — The Unit has either requested the project/initiative be removed from the PA review process or the Privacy Office has administratively withdrawn the PA because it was inactive with the Unit for more than a year. A withdrawn project/initiative can easily be restarted with an email from the Unit POC to SmithsonainPrivacyOffice@si.edu, requesting the project PA review be resumed.
- Approval — The Privacy Office will maintain the completed privacy review documentation in the Archer repository where it will be updated when a project experiences a material change or after a period of three years, whichever comes first.

B. Applying the Smithsonian Privacy Principles to Smithsonian Systems

The Privacy Principles provided in SD 118, Privacy Policy, explain the standards by which the Smithsonian shall create, collect, use, process, store, maintain, disseminate, disclose, and dispose of PII/sPII. As such, they should be leveraged throughout the PA process along with the template questions to ensure the rights of the individual are respected while mitigating privacy risk.

In accordance with the Smithsonian Privacy Principles, Smithsonian Employees and Affiliated Persons should 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 that is, paper) means, Employees and Affiliated Persons should 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.
Prior to a Unit's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII or sPII as part of a new or existing project, program, or initiative implementing a material change that will result in the new creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII and sPII, the Unit is required to obtain prior approval by the SPO, as described in SD 118, Privacy Policy.

In the case of sPII that 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 valid business "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.

During the privacy review and approval process, as defined above, 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 Section 5 on "Guidance for Handling PII and sPII" for supporting procedures.

Similarly, for PII and sPII created, collected, used, processed, stored, maintained, disseminated, disclosed, and 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) to ensure that appropriate technological security controls, protections, and procedures are implemented in accordance with SD 920, IT 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.

C. Privacy Training

All Employees and Affiliated Persons who are provided access to Smithsonian network accounts are required to complete annual Computer Security Awareness Training (CSAT), which currently includes general information for handling and safeguarding Smithsonian data, including PII/sPII. The Privacy Office reviews CSAT annually to provide guidance and updates to the sections which address privacy concerns.

Employees and Affiliated Persons who handle PII as a regular part of their job responsibilities are required to complete role-based privacy training. This training is called Privacy 101 and is available through the Learning Management System. Per a finding from the Office of the Inspector General, the Privacy Office tracks compliance with this training requirement on a Unit-by-Unit basis. Reports on Unit compliance with this requirement may be provided to leadership at the Institution and at the Unit level. If you believe that you have been miscategorized as one who regularly handles PII, please reach out to your Unit IT director so he or she can contact the Privacy Office and modify the Unit list of required persons.

The SPO develops, updates, and delivers 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. To schedule a Unit-specific privacy training session, please reach out directly to the Privacy Office for availability.

D. PII Inventory

In FY 2018, a comprehensive inventory of PII (in paper and electronic formats) was completed on behalf of the Smithsonian. In line with industry guidance and best practices, the inventory will be updated every three to five years. In between updates, revised approved Archer 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 Policy*.

E. Compliance Testing

On March 14, 2016, the Office of Inspector General (OIG) issued its audit of the Smithsonian Privacy Program, *Report on the FY 2015 Independent Audit of the Smithsonian Institution Privacy Program*. In the report, the OIG recommended that the Smithsonian Privacy Officer (SPO) "develop and implement a formal process to periodically test compliance with Smithsonian requirements to safeguard PII [personally identifiable information] in physical form."

In response to this audit recommendation, the SPO developed a self-assessment for Smithsonian Units to complete. Units are sent the self-assessment on a rotating basis and asked to perform walkthroughs of their space to ensure compliance with Smithsonian policy regarding PII/sPII in physical form.

Appendix

A. Exhibit I. Archer Privacy Assessment (PA) Extract and Guidance for IT Systems.

- The Smithsonian Archer PA is conducted in an online automated tool. An extract of the form can be found at: http://prism2.si.edu/SIOrganization/PrivOfc/Documents/Archer%20PA%20Extract%202017-10-27.pdf
- Guidance on how to complete the Archer PA can be found at: http://prism2.si.edu/SIOrganization/PrivOfc/Documents/Archer%20PA%20Guide%20v1.0.pdf
- The above documents as well as FAQs on the Archer PA are maintained on the Privacy Office Prism Page: http://prism2.si.edu/SIOrganization/PrivOfc/Pages/Archer_PA_Guidance.aspx

B. Exhibit II. Archer PA Extract for Paper Systems

Privacy Assessment - Paper Records: 357581

Created Date: 7/18/2019 3:24 PM Last Updated: 7/19/2019 3:21 PM

Instructions

The Requirement to Complete a Privacy Review

Per SD 118, Privacy Policy, 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 personally identifiable information (PII) and sensitive PII (sPII) 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." This requirement applies to all PII and sPII collected by or on behalf of the Smithsonian, regardless of medium (paper, IT system, shared drive, video device, audio recording device, or any other format which can store PII/sPII).

Scope

The following **Privacy Assessment for Paper Records and Non-IT Systems** is designed to be used in cases where PII/sPII is collected, used, stored, or disseminated outside of an Information Technology (IT) system. An Information [Technology] System is defined in IT-930-03, Security Assessment & Authorization, as: ""a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual" (i.e., a set of IT resources organized together to perform a particular function). Examples of systems include, but are not limited to applications, websites, networks, and IT devices."

Examples of non-IT System that should be assessed by this template are:

- Human Subjects Research where all PII/sPII is collected over email or in person and stored on a shared drive/hard drive/laptop or mobile device/locked file cabinet
- Educational programs where permission forms are collected in paper format and audio/video recordings are made of participants
- Human Resources documents that are stored in a shared drive/hard drive/laptop or mobile device/locked file cabinet
- Records on donors that are stored outside of Panda
- Visitor logs that are recorded on a sign-in sheet for security or other purposes
- Receipts that are stored after a purchase is made where PII or sPII is visible

For More Information

Guidance on how to protect and secure PII/sPII in Paper and Non-IT System format can be found in SD 118, *Privacy Program Handbook*. For Frequently Asked Questions (FAQs), and guidance on when and how to complete this assessment please visit our Privacy Assessment for Paper Records and Non-IT Systems Information Portal on Prism. All other questions should be addressed to SmithsonianPrivacyOffice@si.edu.

General Information

Authorization Package

Unit Name
OCIO - Office of Chief Information Officer

Questionnaire ID:		**Overall Status:**	In Process
PA Name:	Privacy Test	**Type of Paper**	Administrative/Personnel & Human Resources

		Record/Non-IT System Category :	
Mission/ Purpose:			

Previous Privacy Assessment Documents

Document Name
No Records Found

Due Date:		**History Log:**	**View History Log**

Workflow

Submitter:	Goodyear, Eva	**Submission Status:**	In Process
Unit Director:	Burba, Deron	**Submit Date:**	
Initial Reviewer:	Goodyear, Eva	**Initial Review Status:**	No Selection
Initial Review Start Date:		**Initial Review Date:**	
Final Reviewer:	Gaines Adams, Danee	**Final Review Status:**	No Selection
Final Review Start Date:		**Final Review Date:**	
Additional Info Required:			
Reviewer Comments:			

PA 1: General Privacy Information

PA 1-1:	**General PII** (select or list all the elements of PII that will be collected into the system):	First Name Middle Name Last Name Other names used Mother's maiden name Gender Birth date/age Religion Race/ethnicity Place of birth Marital status Citizenship Education information

		Financial information
		Disability information
		Family information
		Medical information
		Military service information
		Employment information (incl. grade and history)
		Photo, video, and/or audio recording
		Biometrics (e.g. fingerprints and DNA) apart from photo, video, audio recordings
		Clearance information
PA 1-2:	**Contact PII** (select or list all the elements of PII that will be collected into the system):	Personal mailing address
		Personal e-mail
		Personal telephone number
		Office mailing address
		Office e-mail
		Office telephone number
PA 1-3:	**Identifying numbers** (select or list all the elements of PII that will be collected into the system):	Social Security Number
		Truncated SSN (last 4)
		Other taxpayer ID
		Smithsonian ID number
		Passport number
		Driver's license number
		Credit card number
		Other financial number
		Other government issued ID number (e.g. Panamanian ID Number)
PA 1-4:	**Spouses/partners** (select or list all the elements of PII that will be collected into the system):	Name
		Contact information
		Relationship
PA 1-5:	**Children/dependents** (select or list all the elements of PII that will be collected into the system):	Name
		Contact information
		Relationship
PA 1-6:	**Emergency contacts** (select or list all the elements of PII that will be collected into the system):	Name
		Contact information
		Relationship
PA 1-7:	Does this system collect any information relating to residents of the European Union? If yes, please list that information here:	
PA 1-8:	List any other PII that will be collected into the system:	

PA 1-9:	Please select this box if this system does not include any PII (i.e. PA 1-1 through PA 1-8 are all blank):	

PA 2: PII from Smithsonian Employees

PA 2-1:	Does all the PII collected about **Smithsonian Employees** come from Active Directory (i.e. the Outlook Global Address Lookup or the PRISM Staff Directory)?	No
PA 2-1-1:	Describe the **Smithsonian Employees** whose PII will be collected into this system:	
PA 2-1-2:	Approximately how many **Smithsonian Employees** will have their PII in this system:	1000
PA 2-1-3:	Explain all the PII that will be collected about these **Smithsonian Employees:**	
PA 2-1-4:	Select one or both of the following regarding **Smithsonian Employees'** ability to consent (opt-in) to the collection and/or use of their PII:	Smithsonian Employees will be asked for their consent (opt-in) before their PII is collected and/or used.
PA 2-1-4-1:	When will **Smithsonian Employees** have an opportunity to consent (opt-in) to the collection and/or use of their PII:	
PA 2-1-4-2:	How will **Smithsonian Employees** consent (opt-in) to the collection and/or use of their PII:	
PA 2-1-4-3:	What will happen if **Smithsonian Employees** do not consent (opt-in) to the collection and/or use of their PII:	
PA 2-1-5:	Select one or both of the following regarding **Smithsonian Employees'** ability to decline (opt-out of) the collection and/or use of their PII:	Smithsonian Employees will be able to decline (opt-out of) the collection and/or use of their PII.
PA 2-1-5-1:	When will **Smithsonian Employees** have an opportunity to decline (opt-out of) the collection and/or use of their PII:	
PA 2-1-5-2:	How will **Smithsonian Employees** decline (opt-out of) the collection and/or use of their PII:	
PA 2-1-5-3:	What will happen if **Smithsonian Employees** decline (opt-out of) the collection and/or use of their PII:	
PA 2-1-6:	Will this system collect full or truncated (partial) SSNs about **Smithsonian Employees**?	Yes
PA 2-1-6-1:	This system will collect and/or use (please select one or more of the following):	Truncated SSNs
PA 2-1-6-2:	How will full and/or truncated SSNs be collected and/or used:	
PA 2-1-6-3:	Explain why another identifier will not be collected and/or used instead:	
PA 2-1-6-4:	Explain any future plans to eliminate the collection and/or use of the full and/or truncated SSNs:	

PA 3: PII from Affiliated Persons

PA 3-1:	Will PII about **Affiliated Persons** be collected into the system?	CONTRACTORS who perform work similar to Smithsonian employees, such as employees of temporary help firms/companies. VOLUNTEERS.

		INTERNS as defined in and . FELLOWS, as defined in and . VISITING RESEARCHERS, including scientists, scholars, and students. RESEARCH ASSOCIATES, as defined in . EMERITI, as defined in REGENTS AND ADVISORY BOARD MEMBERS. FRIENDS OF THE NATIONAL ZOO (FONZ), ITS EMPLOYEES, AND VOLUNTEERS. SMITHSONIAN EARLY ENRICHMENT CENTER (SEEC) EMPLOYEES EMPLOYEES OF FEDERAL, STATE, AND LOCAL AGENCIES working in or on Smithsonian facilities and property EMPLOYEES OF THE GOVERNMENT OF PANAMA working at the Smithsonian Tropical Research Institute (STRI).
PA 3-1a:	Describe the contractors:	
PA 3-1b:	Describe the volunteers:	
PA 3-1c:	Describe the interns:	
PA 3-1d:	Describe the fellows:	
PA 3-1e:	Describe the visiting researchers:	
PA 3-1f:	Describe the research associates:	
PA 3-1g:	Describe the emeriti:	
PA 3-1h:	Describe the regents and advisory board members:	
PA 3-1i:	Describe the FONZ, employees, and volunteers:	
PA 3-1j:	Describe the SEEC employees:	
PA 3-1k:	Describe the employees of federal, state, and local agencies:	
PA 3-1l:	Describe the employees working at STRI:	
PA 3-1-1:	Approximately how many **Affiliated Persons** will have their PII in this system (specify by type of Affiliated Person):	
PA 3-1-2:	Explain all the PII that will be collected about the **Affiliated Persons** (specify by type of Affiliated Person):	
PA 3-1-3:	Select one or both of the following regarding the **Affiliated Persons'** ability to consent (opt-in) to the collection and/or use of their PII?	In some or all situations, Affiliated Persons will be asked for their consent (opt-in) before their PII is collected and/or used.
PA 3-1-3-1:	When will the **Affiliated Persons** have an opportunity to	

	consent (opt-in) to the collection and/or use of their PII:	
PA 3-1-3-2:	How will the **Affiliated Persons** consent (opt-in) to the collection and/or use of their PII:	
PA 3-1-3-3:	What will happen if the **Affiliated Persons** do not consent (opt-in) to the collection and/or use of their PII:	
PA 3-1-4:	Select one or both of the following regarding the **Affiliated Persons'** ability to decline (opt-out of) the collection and/or use of their PII?	In some or all situations, Affiliated Persons will be able to decline (opt-out of) the collection and/or use of their PII.
PA 3-1-4-1:	When will the **Affiliated Persons** have an opportunity to decline (opt-out of) the collection and/or use of their PII:	
PA 3-1-4-2:	How will the **Affiliated Persons** decline (opt-out of) the collection and/or use of their PII:	
PA 3-1-4-3:	What will happen if the **Affiliated Persons** decline (opt-out of) the collection and/or use of their PII:	
PA 3-1-5:	Will this system collect full or truncated (partial) SSNs about the **Affiliated Persons**?	No

PA 4: PII from Members of the Public or Other Individuals

PA 4-1:	Will PII about **Members of the Public or Other Individuals** be collected into this system?	Yes
PA 4-1-1:	Describe the **Members of the Public or Other Individuals** whose PII will be collected into this system:	
PA 4-1-2:	Approximately how many **Members of the Public or Other Individuals** will have their PII in the system:	1000
PA 4-1-3:	Explain all the PII that will be collected about the **Members of the Public or Other Individuals**:	
PA 4-1-4:	Select one or both of the following regarding the **Members of the Public or Other Individuals'** ability to consent (opt-in) to the collection and/or use of their PII:	Members of the Public or Other Individuals will be asked for their consent (opt-in) before their PII is collected and/or used.
PA 4-1-4-1:	When will the **Members of the Public or Other Individuals** have an opportunity to consent (opt-in) to the collection and/or use of their PII:	
PA 4-1-4-2:	How will the **Members of the Public or Other Individuals** consent (opt-in to the collection and/or use of their PII:	
PA 4-1-4-3:	What will happen if the **Members of the Public or Other Individuals** do not consent (opt-in) to the collection and/or use of their PII:	
PA 4-1-5:	Select one or both of the following regarding the **Members of the Public or Other Individuals'** ability to decline (opt-out of) the collection and/or use of their PII:	Members of the Public or Other Individuals will be able to decline (opt-out of) the collection and/or use of their PII.
PA 4-1-5-1:	When will the **Members of the Public or Other Individuals** have an opportunity to decline (opt-out of) the collection and/or use of their PII:	
PA 4-1-5-2:	How will the **Members of the Public or Other Individuals** decline (opt-out of) the collection and/or use of their PII:	
PA 4-1-5-3:	What will happen if the **Members of the Public or Other Individuals** decline (opt-out of) the collection and/or use of their PII:	

PA 4-1-6:	Will this system collect full or truncated (partial) SSNs about the **Members of the Public or Other Individuals**?	No

PA 5: Collections of PII Directly From Individuals

PA 5-1:	Will this system collect PII directly from individuals:	Yes
PA 5-1-1:	Explain the PII that will be collected directly from individuals:	
PA 5-1-2:	From whom will the PII be collected:	
PA 5-1-3:	How will PII be collected directly from individuals (select all that apply):	In person
		Audio recordings
		Websites/onsite software
		Telephone
		Video recordings
		E-mails
		Paper (mail/fax)
		Still cameras
		Forms/surveys
PA 5-1-4:	Will any forms/surveys be used to collect the PII directly from individuals:	No
PA 5-1-5:	When PII is collected directly from individuals will a privacy notice be provided?	Yes
PA 5-1-5-1:	Explain when and how privacy notices will be provided:	
PA 5-1-5-2:	Upload a copy of the privacy notices:	
PA 5-1-6:	Are there any situations where PII will be collected directly from individuals and a privacy notice will NOT be provided?	
PA 5-1-7:	Will this system involve human subject research?	Yes
PA 5-1-7-1:	Has approval been obtained from the Office of Sponsored Projects?	Yes

PA 6: Collections of PII from Other Systems

PA 6-1:	Will this system obtain PII from other systems?	Yes
PA 6-1-1:	For each system that will feed into this system, provide: 1) The name of that system; 2) What PII will be acquired from that system; and 3) Who owns that system (e.g. which federal agency, public company, or private company):	
PA 6-1-2:	Are any of the systems owned by the Smithsonian?	
PA 6-1-3:	Are any of the systems owned by a federal agency?	

PA 7: Access to PII

PA 7-1:	What categories of individuals will have access to the PII in this system and why:	

PA 7-2:	Approximately how many individuals will be in each category listed above:	
PA 7-3:	Will those individuals have access to all PII or a limited set:	
PA 7-4-1:	Select one of the following answers:	All individuals with access to PII will receive training or rules of conduct before accessing the system.
PA 7-4-1-1:	Explain the training or rules of conduct:	
PA 7-4-1-3:	Upload a copy of the training or rules of conduct:	

PA 8: Sharing and Disclosures of PII

PA 8-1:	Will PII stored/maintained in this system be shared or disclosed outside of this system?	Yes
PA 8-1-1:	For each entity that will receive PII from this system, provide: 1) A description of that entity; 2) A list of what PII that entity will receive (all or what subset); and 3) Explain why that entity will receive the PII:	
PA 8-1-2:	Will PII in this system be shared with, or disclosed to, one or more Smithsonian systems?	
PA 8-1-3:	Will PII in this system be shared with, or disclosed to, one or more federal systems?	

PA 9: Physical, Administrative, and Technical Controls

PA 9-1:	Select and/or explain the physical controls employed by this system (select all that apply):	Security guards Combination Locks Locked File Cabinets Facility access Controls Cipher locks Key cards Safes Identification Cards Closed Circuit TV (CCTV)
PA 9-1a:	Select and/or explain the administrative controls employed by this system (select all that apply):	Periodic security audits Breach response policy Training Periodic Privacy Audits (Walk-throughs to test compliance with policy)

PA 10: Data Storage and Retention

PA 10-1:	Where will the information collected into this system be stored? Please list all locations and the approximate volume at each location:	

PA 10-2:	In total, across all locations listed above, how many unique entries, or records, of individuals are in the system?	1,001-5,000
PA 10-3:	Select one or both of the following concerning retention schedules:	The PII stored/maintained in this system is NOT governed by a retention schedule.
PA 10-3-2:	Explain why some or all of the PII will not be subject to a retention schedule:	

PA 11: PCI DSS Compliance Information

PA 11-1:	Will this system contain credit card PII? If yes, please work with John Duven (DuvenJ@si.edu) to meet Payment Card Industry (PCI) requirements for paper records/non-IT systems.	Yes
PA 11-1-1:	Date that the current PCI DSS compliance evaluation will end:	
PA 11-1-2:	Date that the next PCI DSS compliance evaluation will begin:	

PA 12: Information on 3rd Party Vendors

PA 12-1:	Will this system be supported or accessed by one or more non-Smithsonian (non-SI) parties (e.g. vendors) who will have access to the PII stored within this system?	Yes
PA 12-1-1:	Provide the name and role of each non-SI party:	
PA 12-1-2:	Select from the following options concerning the relationship between the Smithsonian and any third party (select all that apply):	One or more of the non-SI parties will have an agreement with the Smithsonian.
PA 12-1-3:	Will any of the non-SI parties have Smithsonian network or system access?	Yes
PA 12-1-3-1:	List the non-SI parties who will have Smithsonian network or system access.	
PA 12-1-4:	Will all of the non-SI parties have Smithsonian badges?	Yes
PA 12-1-5:	Will any of the non-SI parties store/maintain PII on behalf of the Smithsonian?	Yes
PA 12-1-5-1:	List the non-SI parties that will store/maintain PII on behalf of the Smithsonian. What PII will be stored/maintained, and how it will be safeguarded?	
PA 12-1-5-2:	Will the non-SI parties be required to return the PII at the expiration/termination of the contract?	Yes
PA 12-1-5-3:	Will the non-SI parties be required to destroy the PII at the expiration/termination of the contract?	Yes
PA 12-1-5-4:	Will a 3rd party certify that the non-SI parties destroyed the PII?	Yes

PA 13: Additional Privacy Concerns

PA 13-1:	Do you publicly state whom individuals should contact if they have a question about this system?	Yes

PA 13-1-1:	Where is that contact information provided:	
PA 13-1-2:	Please provide that contact information here:	
PA 13-2:	How will the Unit assure that PII in this system is accurate, relevant, timely, and complete:	

PA 17: Data Collections from Children and SD 124

PA 17-1:	Are you collecting any releases or permission forms from parents or legal guardians like the kind described in SD 124, Protection of Minors? For example, forms that give SI permission to photograph a child or give a child permission to attend an event?	Yes
PA 17-1-1:	Describe the: • Event this information is being collected for; • Age range of the minors; and • PII collected about the minors:	
PA 17-1-2:	Upload the registration forms, release forms, consent forms, or other forms like the kind described in SD 124:	

PA 18: Data Collections from Children and the SKOP

PA 18-1:	Select yes if this project: • is designed to collect children's PII (purposely) and/or • will end up collecting children's PII even if not intentionally (knowingly):	No
PA 18-1-2-1:	Upload the notice that will explain the collections, uses, and disclosures of the children's PII:	
PA 18-1-2-2:	Is this notice part of the Kid Site's FAQs, Rules, or Usage Terms?	Yes
PA 18-1-2-3:	Will a link to this notice be present on the Kid Site's home page or equivalent?	Yes
PA 18-1-2-4:	Will a link to this notice be present wherever children's PII will be collected through the Kid Site?	Yes
PA 18-1-4-1:	Will every page of each Kid Site include a link to the Smithsonian Institution's Privacy Statement?	Yes
PA 18-1-4-1-1:	Where will the links be located?	
PA 18-1-4-2:	Will every page of each Kid Site include a link to the Smithsonian Institution's Terms of Use?	Yes
PA 18-1-4-2-1:	Where will the links be located?	
PA 18-1-4-3:	Will every page of each Kid Site include a link to the SKOP Statement?	Yes
PA 18-1-4-3-1:	Where will the links be located?	
PA 18-1-4-4:	Does this website include site-specific Usage Terms, Rules, or FAQs?	Yes
PA 18-1-4-4-1:	Upload site-specific Usage Terms, Rules, or FAQs:	

PA 19: Additional Information

	Please share any additional background or context that would	

PA 19-1:	help the Privacy Office understand your system.	
PA 19-2:	Please upload any other documents that would help the Privacy Office understand your system.	

PA 20: Coordination

PA 20-1:	Are you working with one or more people in the Office of Sponsored Projects (OSP) for Human Subjects Research?	Yes
PA 20-1-1:	Name of the individual(s) in OSP:	
PA 20-2:	Have you communicated with SIA Records Management about a disposition schedule for the information in this system:	Yes
PA 20-2-2:	Name of the individual(s) in SIA Records Management:	
PA 20-3:	Have you worked with someone (1) in the Office of Contracts, (2) in the Office of General Counsel, or (3) a Unit Procurement Officer on an agreement related to this system (e.g. contract, purchase order):	Yes
PA 20-3-1:	Name of the individual(s):	