



National Park Service  
U.S. Department of the Interior

Natural Resource Stewardship and Science

---

# **GRSM Standard Operating Procedure: Sensitive Data Handling**

Suggested Citation: National Park Service. 2016. GRSM Standard Operating Procedure: Sensitive Data Handling. Version 2016-07-20. National Park Service, Great Smoky Mountains National Park. Gatlinburg, Tennessee.

## Contents

|                                      |    |
|--------------------------------------|----|
| Purpose.....                         | 3  |
| Scope .....                          | 3  |
| Introduction .....                   | 3  |
| Managing Protected Information ..... | 3  |
| Roles and Responsibilities.....      | 10 |
| Acronyms and Definitions .....       | 10 |
| Contact Information .....            | 10 |
| References .....                     | 11 |

| Version History |             |                                     |
|-----------------|-------------|-------------------------------------|
| Version         | Update Date | Changes                             |
| 20160719        | 20160719    | Revised draft to appropriate format |
|                 |             |                                     |
|                 |             |                                     |
|                 |             |                                     |

## Purpose

This document summarizes the legal requirements related to protected information and describes procedures for classifying and managing protected information. Much of the following material is derived from NPS Director's Order #66B: Freedom of Information Act and the Protection of Exempted Information (Draft).

## Scope

These guidelines apply to all GRSM (Great Smoky Mountains National Park) staff, cooperators, contractors, and other partners, regardless of whether they are park-funded or not, who are likely to obtain or have access to information about protected NPS resources. The NPS principal investigator in collaboration with the data manager and GIS specialist has primary responsibility for ensuring adequate protection of sensitive information related to the project.

## Introduction

Although it is NPS policy to share information widely, the NPS also realizes that providing information about the location of park resources may sometimes place those resources at risk of harm, theft, or destruction. This can occur, for example, with regard to caves, archeological sites, tribal information, and rare plant and animal species. Therefore, information will be withheld when the NPS foresees that disclosure would be harmful to an interest protected by an exemption under the Freedom of Information Act (FOIA). The Department FOIA policy is generally to release as much information as possible without releasing too much, and to segregate releasable information from non-releasable information.

The National Parks Omnibus Management Act (NPOMA), Section 207, 16 U.S.C. 5937, is interpreted to prohibit the release of information regarding the "nature or specific location" of certain cultural and natural resources in the national park system. Additional details and information about the legal basis for this policy can be found in the NPS Management Policies (National Park Service 2006), and in Director's Order #66.

## Managing Protected Information

The principal investigator will work closely with the park data manager and GIS specialist on all projects to ensure potentially sensitive park resources are identified and information about these resources is tracked throughout the project. The investigators, whether NPS staff or partners, will develop procedures to flag all potentially sensitive resources in any products that come from the project, including documents, maps, databases and metadata. All records and other references to the potentially sensitive resources should be specifically identified by the investigator when submitting any products. Park staff, individual volunteers, and park partners should not release any information before consulting with appropriate resource management staff to ensure that the information is not classified as protected. The following definitions are pertinent to subsequent sections:

- *Protected resources* are defined as:
  - o species that have State- or Federally-listed status of any kind;
  - o other species deemed rare or sensitive to loss by local park taxa experts. These include any species "...that occurs in low enough numbers or small enough area of distribution that it could disappear from the park" (D.O.66b).
    - These taxa are identified on a park-maintained list within the NPSpecies system.
  - o some cultural resources also warrant protection.
- *Sensitive information* is defined as
  - o information about protected resources which may reveal the "nature or specific location" of protected resources;
  - o information that would enable non-NPS employees to locate protected resources (e.g. manways);
  - o information that Visitor Protection requires for its mission (e.g Radio Coverage);

- o information that, if used by non-NPS staff, could result in harm or death to the user;
- o Such information must not be shared outside the National Park Service, unless a signed confidentiality agreement is in place, and that agency or organization has the legal means to keep information confidential.;
- o Information that has been identified as “For Official Use Only” in the metadata or Access and Use Constraints section of data discovery portal.

### ***How to evaluate resources for protection?***

The classification of protected natural and cultural resource information from GRSM will be done on a case-by-case, project-by-project basis. According to NPOMA, if NPS determines disclosure of information would be harmful, information may be withheld concerning the nature and specific location of:

- Endangered, threatened, rare, or commercially valuable NPS resources
- Mineral or paleontological objects
- Objects of cultural patrimony

The Federal Cave Resources Protection Act (16 U.S.C. § 4304) similarly authorizes the withholding of information concerning the specific location of any significant caves. It is park policy that no location information about caves or abandoned mines is released publically.

Section 304 of the National Historic Preservation Act (NHPA) (16 U.S.C. 470) requires that information about the location, nature or ownership of historic resources be withheld from disclosure to the public if that disclosure may cause a significant invasion of privacy, risk harm to the historic resource, or impede the use of a traditional religious site by practitioners. Historic resources as defined by the NHPA are any “prehistoric or historic district, site, building, structure or object included in or eligible for inclusion on the National Register of Historic Places, including artifacts, records, and material related to such a property or resource.”

Section 9 of the Archaeological Resources Protection Act of 1979 (APRA) (16 U.S.C.) directs federal agencies to withhold information about the nature and location of any archaeological resource for which the excavation or removal requires a permit or other permission under federal law unless disclosure would further the purposes of ARPA or the Reservoir Salvage Act or that it would not create a risk of harm to such resources or to the site at which such resources are located.

The following questions should be considered in determining the possibility for an unreasonable risk of harm, theft, or destruction to occur:

- Has harm, theft, or destruction occurred to a similar resource on federal, state, or private lands?
- Has harm, theft, or destruction occurred to other types of resources of similar commercial value, cultural importance, rarity, or threatened or endangered status on federal, state, or private lands?
- Is information about locations of the park resource in the park specific enough so that the park resource likely could be found at these locations at predictable times now or in the future?
- Would information about the nature of the park resource that is otherwise not of concern permit finding the resource if the information were available in conjunction with other specific types or classes of information?
- Even where relatively outdated, is there information that would reveal locations or characteristics of the park resource such that the information could be used to find the park resource as it exists now or is likely to exist in the future?
- Does NPS have the capacity to protect the park resource if the public knows its specific location?
- Has the level of risk changed? The NPS may withhold information about the nature and location of historic resources if that information has changed since its previous release. Or some historic

resources may be at increased risk after 9/11 and previously released information on these historic resources may now warrant being withheld.

If upon review by a subject matter expert (either internal or external) a sensitivity designation changes that change as well as the rationale are documented in the NPSpecies system. Generally, the date, contact information and reasoning are recorded for each designation change. This documentation provides useful context for our decision making.

### ***What information do we release?***

Releasing information refers to the sharing of information outside of the NPS via NPS Data Store, publications, reports, peer to peer dissemination of information, or other means of information distribution (see the GRSM Data Dissemination SOP for more information). Data sets that contain sensitive information should be published in Data Store in redacted form or in total with limited access. The Data Store reference should always be visible to the public; however, the associated data sets can be limited to internal distribution to appropriate audiences.

Project staff and cooperators must not release:

- Specific location of a protected resources (without appropriate modification—see next section) including the following:
  - o Coordinates – in any form, UTM's, Lat-Long, state plane grid, etc
  - o Any location metadata that would allow someone to specifically locate the protected resource. Depending on the project this may include:
    - Travel descriptions
    - Place names
    - Elevations
    - Descriptions of specific habitats
    - Other fields that contain information which may reveal the specific location of the protected resource(s)
- Protected resource observations at disclosed location—if specific location information has already been made publicly available, the occurrence of protected resources at that location cannot be shared outside NPS without a confidentiality agreement.
  - o E.g., if a sensitive species is observed at an already disclosed (via the Data Store, publication or otherwise) monitoring site; the observation must be redacted from the dataset and cannot be referred to in any reports, publications etc. outside the NPS
- In rare instances, acknowledgment that a particular resource exists in the park may effectively reveal its location
  - o E.g., if there is only one perennial standing water source in a military park, and that pond provide habitat for a listed frog, acknowledging the existence of the frog in the park would provide sufficient information to locate it.
- Location information identifying a resource in such a manner that navigation to the resource is considered hazardous

Project staff and cooperators can release:

- All information about the protected resource that does not reveal details about its nature or specific location.

### ***Sharing Sensitive Information***

No sensitive information may be shared outside NPS without a confidentiality agreement (see Cooperative Agreement and Confidentiality Agreement section for more detail) between NPS and the

agency, organization, or person(s) with whom the sensitive information is to be shared. Only products intended for public/general-use may be posted to public websites and clearinghouses – these may not contain sensitive information. Note: the NPS Data Store allows users to constraint access to flag references as containing sensitive information, such references and their associated holdings will only be internally (NPS) accessible. ***Distribution of approved sensitive information may only occur through approved NPS technology channels (e.g. Secure FTP).***

### ***Modifying Sensitive Data for Release***

In the context of releasing as much information as possible, but not too much, products containing sensitive information may require modification before release. Acceptable forms of modification include 1) redacting observations of protected resources and 2) generalizing or “fuzzing” location data.

*Redacting observations of protected resources* in circumstances in which leaving location data intact but removing a minimal number of observations is appropriate. For example, many protocols require the recording of the vegetative community. In many cases a few rare species will be observed. These records can easily be removed from the dataset without undue compromise of its interpretability.

*Generalizing or “fuzzing” location data* allows investigators to implement location granularity to the data to an area large enough so that a requester has some level of information without knowing the specific location of a park resource that could make it susceptible to harm, theft, or destruction. The degree of generalization is up to the subject matter expert and depends on several factors including species life history and viability, ability of discern specific habitat for the species, and potential threat to the species, among other factors. Depending on these factors varying levels of generalization may be appropriate including replacing the last digits in UTM coordinates with zeros, only specifying county, or only specifying watershed. This generalization extends to text descriptions of locations and other relevant metadata that may reveal the nature and specific location of a protected resource. The Data Manager and/or GIS Specialist will provide technical assistance as needed to edit data products for sensitive information.

### ***Working with collaborators***

#### ***Federal***

NPS often enters into information-sharing agreements with other federal agencies to facilitate scientific study. The NPS should notify these federal agencies that protected information must be withheld under resource confidentiality laws and the Executive Order applicable to park resources. In general, any federal agency that holds information about the nature and specific location of park resources that qualifies as protected information must withhold that information from the public. Specific information regarding procedures for handling FOIA requests while in an information-sharing agreement can be found in Director's Order #66B.

Note ARPA provides an exception requiring federal land managers to release information about the nature and location of archaeological resources in a state upon a governor's written request and commitment to protect the information.

#### ***State***

Before sharing information with state employees, whether from state agencies or state funded universities, NPS must be aware that those state employees may be obligated to release information in their possession to any party requesting it due to state freedom of information or sunshine laws requiring such release. Some such state laws allow the withholding of certain types of information and it may be possible that state employees would have the authority to enter into contractual agreements with the NPS to withhold protected information. NPS must not share protected information with any state employee

where state laws require the release of all information in state records. GRSM should not create confidentiality agreements or share sensitive information with agencies in North Carolina or other states with sunshine laws without first seeking the advice of an NPS solicitor. Under § 11-1-102(2012), Tennessee has provided protection against the disclosure of the location of threatened, endangered, or rare species. To check sunshine laws you can utilize the following website:  
[http://ballotpedia.org/State\\_sunshine\\_laws](http://ballotpedia.org/State_sunshine_laws)

### **Cooperative Agreements and Confidentiality Agreements**

Confidentiality agreements may be created between NPS and another organization or individual to ensure that protected information (either obtained from GRSM, or generated by the requesting organization) is not inadvertently released. Often Confidentiality Agreements can be embedded within a Resource Activity Permit if it involves researchers. The rights and responsibilities of the NPS and partners regarding potentially sensitive park resources should be stated clearly in any Cooperative Agreement, contract, Interagency Agreement, VIP agreement, task agreement or other written confirmation of a working relationship (see GRSM Data Contract Standards). Each agreement should address the following:

- Clarification of the ownership of data and associated information— such as the following text. Note that Federal ownership of information means the information is subject to public release through FOIA.

*“All associated data (including, but not limited to field notes, maps, slides, photographs, charts/graphs, tabular and GIS data with associated metadata) are required to be submitted to the Park annually and are owned by the National Park Service.”*

- Names of all known potentially sensitive park resources— since the agreement itself is a public document only the names of the resources should be provided, not specific information about their distribution or abundance, in case that information should be protected.
- Summary of procedures and responsibilities for classification of protected information (see next section) — especially with regard to cooperation between the park staff and the project staff.
- A requirement for the partner to withhold protected information in perpetuity and to consult with the NPS before releasing any information on sensitive park resources— the following confidentiality agreement is recommended:

*“I agree to keep confidential any protected information that I may develop or otherwise acquire as part of my work with the National Park Service. I understand that with regard to protected information, I am an agent of the National Park Service and must not release that information. I also understand that by law I may not share protected information with anyone through any means except as specifically authorized by the National Park Service. I understand that protected information concerns the nature and specific location of endangered, threatened, rare, commercially valuable, mineral, paleontological, or cultural patrimony resources such as threatened or endangered species, rare features, archeological sites, museum collections, caves, fossil sites, gemstones, and sacred ceremonial sites. Lastly, I understand that protected information must not be inadvertently disclosed through any means including websites, maps, scientific articles, presentation and speeches.”*

- Data will be maintained by the cooperator for the duration of the project and then removed from their systems. If the cooperator or contractor has a need to maintain possession of this data beyond the terms of the project, written permission must be obtained from GRSM.

If agreements do not contain specific responsibilities for the NPS and the partner regarding protected information, then park staff must work with partners to institute appropriate procedures.

### **Responding to Data Requests**

If requests for distribution of products containing sensitive information are initiated by the NPS, by another

federal agency, or by another partner organization (e.g., a research scientist at a university), the unedited product (e.g., the full data set that includes sensitive information) may only be shared after a confidentiality agreement is established between NPS and the agency, organization, or person(s) with whom the sensitive information is to be shared. All data requests will be tracked. **Park staff are not to respond to sensitive data requests on their own initiative under any circumstance. Sensitive data requests are fulfilled by the Data/GIS Manager and reviewed and approved by the RMS Division Chief or designee.**

Once a confidentiality agreement is in place, products containing sensitive information may be shared following these guidelines:

- The text file included with the products should also specify which file(s) contain sensitive information.
- If the products are being sent on physical media (e.g., CD or DVD), the media should be marked in such a way that clearly indicates that media contains sensitive information provided by the National Park Service.
- Always clearly indicate in accompanying correspondence that the products contain sensitive information, specify which products contain sensitive information, and indicate that products containing sensitive information should be stored and maintained separately from non-sensitive information and protected from accidental release or re-distribution. Below is some example language to be included in correspondence.

*"Protecting these data is of the utmost importance. You must take steps to protect these data against accidental release, for example storing a thumb drive with the data in a computer you leave unattended, or saving the data in a folder easily accessed by others in your department etc. We advise that you work with your IT department to come up with a secure solution. In the park for example, we lock folders containing sensitive data and only grant permission to specific individuals. We also encrypt our thumb drives. If you need any guidance as to how to secure this information and all products related to it, please contact us and we can work with you to find a solution. We recommend that you destroy the data when you are no longer utilizing it to minimize the risk you of you losing track of it over time as we will always be required to track this dataset and protect it.*

*Note: You have agreed, by signing the confidentiality agreement embedded within the Research Permit that you will not release the location (specific or otherwise) of these species. This is considering a legally binding document. The sensitive information must be sequestered from other, widely available files on your network/server. You should store this information separately from non-sensitive information and protect against accidental release or re-distribution. This level of protection must continue in perpetuity.*

- Indicate that NPS retains all distribution rights; copies of the data should not be redistributed by anyone but NPS.  
*"NPS retains all distribution rights; copies of the data should not be redistributed by anyone but NPS. Any FIOA (Freedom of Information Acts) requests should be forwards to NPS for handling according to NPS policy."*
- All data, files, and content produced for, by, or in conjunction with the National Park Service which contains **sensitive or rare species information** including location and observation data will be access-controlled with the following statement:  
*"Species location data in this file are considered to be confidential by the National Park Service. The National Park Service has been granted discretionary authority by section 207 of the National Parks Omnibus Management Act of 1998 (16 U.S.C. § 5937) to withhold information from the*

*public “concerning the nature and specific location of a National Park System resource which is endangered, threatened, rare, or commercially valuable.” Some Species Referenced in this database are Fully Protected by the States of North Carolina or Tennessee, and populations of these species occur in limited areas within the Great Smoky Mountains National Park. Because of their status and rarity, the National Park Service exercises its discretion to withhold specific location information about these species from public release pursuant to authority granted within 16 U.S.C. § 5937.”*

- All data, files, and content produced for, by, or in conjunction with the National Park Service which contains **cultural or archaeological data** including location and observation data will be access-controlled with the following statement:

*“Release of locational information for cultural resources are subject to the provisions of Section 304 of the National Historic Preservation Act as Amended and Section (9)(a)(2) of the Archeological Resources Protection Act as Amended.”*

### **Freedom of Information (FOIA) Requests**

All official FOIA requests will be handled according to NPS policy. The NPS Lead will work with the Data Manager and the park FOIA representative(s) of the park(s) for which the request applies.

**Summary of procedures and responsibilities** The procedures for classifying protected information and managing information about sensitive park resources can be summarized as follows:

- Park staff (project leaders, Data Manager, and GIS Specialist) will ensure that all known potentially sensitive park resources are identified
  - Subject matter experts will work with Data Manager to keep sensitive species list up to date
- Project leaders will ensure investigators working on park projects understand that (1) all data and associated information must be made available for review by park staff prior to public release in any format, and (2) any information classified by the NPS as protected should not be released in any format except as specifically coordinated with the NPS.
- Project leaders will provide the principal investigator with a list of potentially sensitive park resources at project initiation.
  - This list is generated from the NPSpecies system and can be provided by the Data Manager upon request
- All known references to potentially sensitive park resources generated from each project, whether internally generated or externally generated, will be identified and properly protected
- Park staff will ensure that all protected information is properly identified and marked before uploading into local or national databases, and before archiving the databases.
  - Data certification provides a means by which the Project Lead and the Data Manager can screen the data set for sensitive information and document the modification of the database prior to dissemination (see the Data Certification SOP).
- Park staff will ensure all references to protected information are removed or obscured in any reports, publications, maps or other public forum.
- Following the standard for FOIA requests, non-releasable information will be segregated. Where practical, releasable information will not be withheld.
- Sensitive data stored on park-owned computers must be protected so that only authorized staff can access the data in order to prevent unauthorized release.
  - IT must be informed of the location of sensitive data on park-owned computers and given a list of who is authorized to access the data. Only a branch chief or higher can manage the access list.

## Roles and Responsibilities

| Role                                                                                      | Responsibility                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Park Employees (General—<br>see previous section for<br>more detail )                     | Recognize and avoid release of protected information.                                                                                                                                                                     |
|                                                                                           | Consult with supervisor and others to determine whether information proposed for release is protected.                                                                                                                    |
|                                                                                           | May share protected information with a partner that has signed a confidentiality agreement.                                                                                                                               |
|                                                                                           | Must not be release protected information unless authorized in writing by the Director or designee.                                                                                                                       |
|                                                                                           | Maintain confidentiality of protected information even after termination.                                                                                                                                                 |
| Partners and Partner Staffs                                                               | Work with park project contact to recognize and avoid release of protected information.                                                                                                                                   |
|                                                                                           | Consult with park project contact to determine whether information proposed for release is protected.                                                                                                                     |
|                                                                                           | May produce and use protected information after signing a confidentiality agreement.                                                                                                                                      |
|                                                                                           | Maintain confidentiality of protected information even after termination of agreement.                                                                                                                                    |
| Research Permit<br>Coordinator/ Science<br>Advisor/ Cultural Resource<br>Manager/ Curator | Obtain contractual agreement from permit holders and researchers to avoid release of protected information. Manage sensitive information in a manner that protect the information from accidental or intentional release. |
| Regional FOIA Officers                                                                    | Advise parks and regional staff on how to avoid the release of protected information consistent with DO 66.                                                                                                               |
| Park GIS Office                                                                           | Implements distribution of sensitive and non-sensitive data and ensures that proper data handling IAW federal law                                                                                                         |

Adapted from 11-09-04 Drafts Reference Manual 66B: Handling Protected Information (National Park Service 2004c) by Mortenson (2005)

## Acronyms and Definitions

**Partners** are individuals or entities that enter into cooperative or collaborative relationships with NPS for the purpose of achieving overlapping goals, where at least some goal is held in common by both the partner and the NPS. This relationship is documented through a letter, VIP appointment, general agreement, permit, contract, or some similar written arrangement. Partners can include both private entities and other federal agencies.

**Protected information** indicates information about a sensitive park resource that must not be released to the public according to any of the four resource confidentiality laws and the Executive Order applicable to NPS.

**Principal Investigator** in this context means the person primarily responsible for the implementation of an inventory or monitoring project, whether that person is a partner, is affiliated with a partner institution, or is an NPS employee.

**Sensitive park resource** indicates a park resource covered by the resource confidentiality laws that is considered susceptible to significant harm, theft or destruction, and about which information should be protected from public release.

## Contact Information

Great Smoky Mountains National Park  
National Park Service

Gatlinburg, TN

Kendra Straub  
Data manager  
(865)436-1703  
Kendra\_Straub@nps.gov

Thomas Colson  
GIS Specialist  
(865)436-1701  
Thomas\_Colson@nps.gov

## References

Boetsch, J.R., B. Christoe, and R.E. Holmes. 2005. Data management plan for the North Coast and Cascades Network Inventory and Monitoring Program. USDI National Park Service. Port Angeles, WA. 88 pp. Retrieved February 6, 2007, from: <http://www1.nature.nps.gov/im/units/nccn/datamgmt.cfm>.

Cook, R.R. 2006. FOIA and Sensitive Data Guidelines. Sierra Nevada Network, U.S. National Park Service, Three Rivers, CA.

Harmon, David, ed. 2006. People, Places, and Parks: Proceedings of the 2005 George Wright Society Conference on Parks, Protected Areas, and Cultural Sites. Hancock, Michigan: The George Wright Society.

Mortenson, D., 2005. Data Management Plan for the Inventory and Monitoring Program, Southwest Alaska Network. United States National Park Service. Anchorage, Alaska. 234 pp.

National Park Service, 2004a. Draft Director's Order #66: Freedom of Information Act and the Protection of Exempted Information. [http://www1.nrintra.nps.gov/DO66/DO\\_66\\_Final\\_Draft.doc](http://www1.nrintra.nps.gov/DO66/DO_66_Final_Draft.doc).

National Park Service, 2004c. Draft Reference Manual RM-66B: Handling protected information. <http://www1.nrintra.nps.gov/DO66/RM-66B-Draft.doc>.

National Park Service, 2004d. Departmental Manual: Freedom of Information Handbook, 383 DM 15. 04/22/2004. United States National Park Service, Washington, D.C.

National Park Service. 2006. Management Policies. Retrieved February 6, 2007, from: <http://www.nps.gov/policy/mp/policies.htm>.