American Planning Association
Planning Advisory Service
Creating Great Communities for All

No. 124

PAS MEMO

Data Governance for Planners

By Norman Wright, AICP

Planning offices are conduits of information. They receive, create, use, and share data from a wide array of sources. This data continues to grow in volume and importance. It has arguably become a planner's most important resource, and planners should manage this resource with the best practices available.

Conventional methods are ready to evolve. Gone are the days of file cabinets, paper reports, and simple spreadsheets saved on a local hard drive. Our data is much more extensive now. It is more sensitive, too. We possess photos of private homes with details about their inhabitants. When a permit is requested, we collect data about the applicant's business interests, some of which must be retained for several years.

There is also valuable custom-made data, unique to the office, that staff develop over many years—often with no reliable backup and no easy way to integrate it into other systems. Indeed, fragmentation might be the most frustrating condition of all. Much of our valuable data is kept in siloed databases, leaving our knowledge base scattered across an archipelago of shared network drives with odd folder names and mismatched formats.

Fragments here, lost reports there, forgotten passwords, unrecognized security risks, valuable reference material on old machines that can be lost with one bad software update…this has become the typical state of data management in the modern planning office. We know we can do better; we know that we should. But how?

This *PAS Memo* explains why good data management must be a fundamental practice for planning offices and provides planners with a clear picture of how planning data management practices can improve through a process known as data governance. Borrowing from the best ideas established in the information technology (IT) industry, this *Memo* contextualizes a basic data governance framework that planners can work to develop in collaboration with other subject matter experts in their greater organizations—a local government, or a private-sector multidisciplinary consulting firm—to meet the specific needs of planning practice.

Data Governance 101

The decisions planners make about data usage can be overwhelming. An overarching data governance practice is necessary.

Data governance refers to the management and control of an organization's information. It encompasses the policies, processes, standards, technologies, and people that ensure data is properly collected, stored, processed, and used in a consistent,

Figure 1. The key elements of a data governance policy structure: goals, principles, data categories, and management standards

secure, and compliant manner. An effective data governance framework includes these key elements:

- **Data governance policies.** Good policies are important in creating a consistent, effective practice. Such policies should establish procedures for how data is collected, stored, accessed, and shared. The policies should create habits and processes that comply with relevant laws and address the elements listed below.
- **Ethical principles.** Planners must always consider the ethical implications of data usage, especially for sensitive or controversial data, and avoid any usage that could cause unintended harm to others. It is important to carefully assess potential risks and benefits before proceeding with data-driven initiatives. The AICP Code of Ethics should serve as a basis for how the rest of the framework is developed; see the sidebar below for a discussion of responsible and ethical data use.
- **Security measures.** These are often established by the organization's IT department. An effective practice will continuously seek better ways to protect information as security needs evolve.
- **Consent and transparency provisions.** When sensitive information is requested (e.g., permit applications, case reports), planners should develop methods to obtain informed consent from individuals before collecting their data. Likewise, transparency requires clear and easily understandable privacy notices that inform users about data practices. Transparency around what data can be and is being shared with third-party vendors or partners is also important and should be reflected in any informed consent request. Agreement templates should require third-party vendors to adhere to similar data protection and privacy standards.
- **Integrity standards.** Data integrity means maintaining accuracy, reliability, and consistency throughout its lifecycle. This is especially critical for legal records, including property records, plats, deeds, and approvals.
- **Retention periods.** Clear data retention policies should specify how long data will be stored and when it will be deleted or anonymized.
- **Auditing and accountability practices.** Regular audits to ensure compliance and identify areas for improvement will strengthen the governance practice. Poor data management holds very real risk, and individuals and departments must be accountable for their data-handling responsibilities.
- **Training and awareness programs.** Data governance requires new terminology and ways of thinking about information. Regular training on the data governance framework for employees and stakeholders will foster a culture of data responsibility within the organization.

Creating and formalizing these practices within an organization will require significant work. Fortunately, the benefits can be realized very quickly. Establishing a data governance practice can create new protections for our residents and clients.

The Importance of Responsible Data Use

Planners must manage their data in a responsible manner. Such information should be handled with a full commitment to the first principle in the AICP Code of Ethics and Professional Practice:

We [as professional planners] shall always be conscious of the rights of others.

Those rights include the right to privacy and protection for any personal information we might collect. The common permit application, for example, requires the applicant's name, address, telephone number, and email address, all considered personal identifiable information (PII) by the U.S. Department of Labor. To handle such data responsibly, planners should preserve the individual's right to privacy by avoiding any further use of the information other than legally or practically required (e.g., a rezoning case involving someone's personal property must share the property address for the sake of accuracy in the public record). Staff reports often include supporting documentation for a public hearing case, including the original application. If the application contains sensitive information that is not legally required to be disclosed, planners should redact that information beforehand.

Such efforts to handle data responsibly are essential for maintaining the community's trust. Responsible practices allow residents to feel confident that their data is being used ethically and encourage them to engage with the planning department willingly.

Responsible data handling also requires a broader sense of how the context of the information can lead to detrimental effects. Many planning offices handle code enforcement cases that include personal information about the residents, property, and nature of the complaint, and this information may remain on a local government's website for several years. We usually share this information in a well-intentioned effort to provide transparency, but this may create unintended consequences. If, for example, such evidence categorizes a person's dwelling as "blight" or labels an accessory dwelling unit as "illegal," the information should be considered sensitive and kept protected until it reaches a public hearing, as these are mere allegations until officially ruled.

Thus, we need to continually refine our definition of what it means to use data responsibly. By upholding ethical standards, planning departments can protect individual rights, foster trust, comply with laws, prevent harm, and still derive valuable information to better serve the public good.

It can also bring renewed focus to the quality and unrealized value of the data we possess and how we might enhance it for more positive results.

This is especially true with the growing use of artificial intelligence (AI), as large language models (LLMs) offer powerful methods for leveraging our data in new ways. With proper data structure and consistent quality, planners can now incorporate data into new models that generate excellent written reports, recommendations, and decision guides that once took weeks to develop. Implementing these new tools requires inputs and data managed with the best practices provided here.

Creating a Data Governance Policy

A data governance practice requires a central organizing policy. The data governance policy should translate goals and objectives into a holistic set of principles that define the standard for how each type of data possessed by the department should be responsibly handled and maintained. The key elements of a policy are a goal statement, core principles, data categories, and data management standards (Figure 1, p. 1). This creates a basic structure that translates the big-picture ideal into the finer details of everyday practice.

Goal Statement

To establish the goal statement, think about the end result: what do we want from this effort? Here is one example:

A comprehensive collection of data that is accurate, secure, protected, integrated, regularly updated, and conveniently available to all as needed.

With the goal statement in place, the next step is developing core principles.

Core Principles

Though every planning department's data governance policy will be based on local context and needs, the following are fundamental principles to address.

- **Structure.** The file plan (see the sidebar on p. 5): its folder structure, naming conventions, version control methods, and integration with access and usage policies.
- **Privacy.** A planning department should protect data that includes personal identifiable information (PII). That includes any data that can be used to identify an individual, such as names, addresses, phone numbers, social security numbers, email addresses, and driver's license numbers. This also includes information that ties individuals to any form of financial information (often related to transactions at the permit counter), civil or criminal records (pertaining to enforcement cases), and any photographs or other images that might be connected to a person's private property.
- **Security.** Security protocols can include rules and guidelines related to logins, passwords and passkeys, verification methods, access rules, and storage requirements. The IT department administers organizational protocols, but additional protections may be needed at the department level. Planners should work with IT to address data backup and recovery, access controls, and encryption. Security also relates to accessibility within the organization; keep sensitive data off global shared drives and institute role-based access controls to ensure that information isn't inadvertently shared with unauthorized persons.
- **Usage rights.** In addition to role-based access controls that make clear who can and cannot see certain types of information, it is equally important to control who can edit information. Collaboration software makes it easier than ever for multiple people to contribute to a work product, and shared network drives allow anyone with internal access to modify unprotected documents. Enforcing a consistent approach to roles, responsibilities, and permissions will preserve data integrity and enhance privacy and security. Staff training may be necessary to help team members understand different access levels and usage rights. Don't forget to establish a protocol for revoking or updating such rights when staff leave the organization or take another role.
- **Integrity.** Data integrity is essential for data quality. A sound governance practice focuses on maintaining data accuracy, reliability, and consistency throughout its lifecycle. Planners should identify and validate any information about legal records. Careful reviews and checkpoints help ensure that only accurate and valid data is accepted into the system. Likewise, auditing and assessment processes enable planners to identify and report errors for correction. Finally, effective and consistent naming conventions and methods for tracking changes to data over time (i.e., version control) are important, as multiple staff will be regularly creating new data.
- **Retention.** Many local governments today are subject to state data retention requirements. If a state statute is lacking in some aspect, establish local standards through administrative policy. Consistent retention policies ensure that data is intelligently managed and volume is minimized responsibly. A reliable starting point is to retain all data related to cases, permit requests, and other official decisions for seven years. The State of Washington's Municipal Research and Services Center offers a toolkit to help local governments develop electronic records retention policies.
- **Auditing and accountability.** Require regular audits for every process and procedure in your governance strategy to ensure your team is adhering to the governance plan. Outside experts should conduct the audits (your IT department can be a valuable resource), though internal audits can also be productive. If something is lacking, the audit should acknowledge the missing piece and document what is being done to resolve it.
- **Sharing agreements.** Planning departments regularly engage in partnerships with third-party service providers. Consult with your organization's procurement team and make sure that requests for proposals and contractual documents incorporate your governance approach.

Third-party partners who use any data from your organization should be subject to the same terms and conditions placed on the department's team. Finally, make clear with both the procurement and IT departments that any data exchanges with third-party groups use the organization's preferred file formats (e.g., .doc, .pdf, .shp, .gdb, .xml, .cvs) and sharing methods (e.g., cloud-based shared drives, physical media drives, email).

- **Third-party data licensing.** Be sure to clarify the ownership and licensing status of any data that is not authored by the organization itself. Some data—such as images sourced from the web—may be protected through copyright law and require a formal licensing agreement before use. Alternatively, data licensed through the Creative Commons may typically be freely used for public educational and awareness purposes, though some restrictions may apply. For any data acquired from a commercial broker (such as Getty Images), planners should ensure the formal licensing agreement is kept on file and add license information to the metadata (found in the file's Properties information) at the time of acquisition. Likewise, for any data extracted from the internet, planners should document its Creative Commons license or other ownership and licensing information in the file's metadata. Existing

Table 1. Basic Data Categories Managed by Planning Departments

Data Type	Description
General client data	Case-specific information related to enforcement cases or permit applications, including proposed plans, subject property details, sketch drawings, photos, staff comments, written and oral testimony, and more. In this category, any personally identifiable information (PII) is redacted from the records.
Sensitive client data	A subset of general client data, this includes any PII in a permit application. Some files, such as a draft case file, will have a redacted copy in the General Client Data category and an unredacted copy in this category.
General correspondence	Email, letters, notifications, chatlogs, voicemails, and other communications that involve any department function.
Sensitive correspondence	A subset of general correspondence, this is any correspondence that includes PII or information related to a nondisclosure agreement (e.g., for a business recruitment effort).
Geospatial data	Maps, aerial imagery, and geographic information system (GIS) data for the city's physical layout, land use, zoning, transportation networks, and infrastructure.
Permit data	Information about ongoing and proposed development projects, building permits, licenses, and construction activities.
Enforcement data	Information about code enforcement violations, including case reports, evidence, notes, and resolutions.
Archival data	Records of past meetings, decisions, agreements, minutes, testimony, and case records.
Demographic data	Information about the city's population, including age, gender, ethnicity, income levels, household size, and educational attainment.
Economic data	Information about the city's economic activities, such as employment statistics, industry sectors, business locations, and commercial development.
Housing data	Information about housing stock, housing affordability, housing permits, vacancy rates, and housing quality.
Transportation data	Information about transportation networks, traffic patterns, public transit usage, road conditions, and transportation infrastructure.
Environmental data	Information about air quality, water quality, green spaces, and environmental conservation efforts.
Land use data	Classification of land areas according to their designated uses, such as residential, commercial, industrial, recreational, or agricultural.
Historical resource data	Information about the city's or a property's historical uses, design, archeology, ownership, and other attributes.
Infrastructure data	Information about the placement and condition of utilities, such as water supply, sewer systems, electricity, and telecommunications.

data files without licensing information, especially images, should be considered nonlicensed and deleted from all databases as part of the auditing process.

Data Categories

Every piece of information planners use, from a staff email thread to the traffic counts in a transportation model, is considered data. The first step in governing this unwieldy mass is to give it structure to better understand what we have. This requires an accounting of existing data—its category, quality, usage, and format. For example, archival data often takes the form of paper records housed in a filing cabinet somewhere in the office. Or perhaps those records have been scanned into PDF documents and are now saved in the cloud. Or perhaps there is a mix of both, as certain states require both paper and digital files to be retained for a specific period.

Data Management 101

The necessary foundation for good data governance is data management. An active data management practice is the best way to prevent all the issues we currently face with unstructured, inconsistent, and incomplete information.

It starts with a **file plan**, which defines the structure, hierarchy, and naming conventions for the data in the shared network drive. It offers an easy, intuitive way to navigate, contextualize, and use all the information the department manages.

The file plan establishes the **folder structure**. A common folder structure for permit applications, for example, will feature distinct categories for each permit type, sorted by year.

The **naming convention** is a crucial part of data management, as file labels provide context on data purpose and content as well as the interrelationships between one file and another. A common naming convention pattern in planning offices is CASETYPE-YYYY-MM-CASE#. For "CASETYPE," a site plan might be "SP," and the CASE# is determined by sequence. So, SP-2024-05-24 would be the 24th site plan submitted in May 2024.

Version control is another important element. Software, for example, runs on version numbers. A shift in software from Version 1.0 to Version 2.0 is considered major, while a shift from Version 2.0 to Version 2.1 is minor. All data should be managed in this fashion. First drafts should be labeled as such, as should final drafts.

As an example, a file plan for a planning office's shared network drive might use the following folder structure, seen when opening the drive:

- Administrative (internal policies or notes from staff meetings)
- Rules, Regulations, and Policies (zoning regulations and municipal codes)
- Public Records (formal decisions, final records of actions taken by the office)
- Permit Cases (information for cases that the office processes)
- Planning Projects (information related to one-time projects)
- Technical Data (information used for analysis, such as Census or GIS data)
- Historical Records (information that is archived after a set time period)

Each folder should have subfolders to further organize the data, with nomenclature depending on local ordinances and policies. For example, the Permit Cases folder might contain the following subfolders:

- Permit Cases
  - Use Permits
  - Building Permits
  - ROW Permits
  - Conditional Use Permits
  - Rezoning Permits
  - Variance Permits

Each of these permit subfolders should have a consistent structure, specified by the file plan, such as the year in which the permit application was accepted:

- Permit Cases
  - Use Permits
    - 2025
    - 2024
    - 2023
    - 2023, etc.

The final level of folders would sort each case by its naming convention, which also serves as its case number:

- Permit Cases
  - Use Permits
    - 2025
      - UP-2025-01-01
      - UP-2025-01-02
      - UP-2025-01-03, etc.

When a permit case is complete and a decision is made, that content will be kept on file as required by the governance plan. The official decision and subsequent ordinance or amendment will be placed in the Public Record root folder at the top of the hierarchy, storing it and all other such decisions with the appropriate archival treatments (i.e., naming conventions, metadata, and security protections).

These are the basics of good data management: consistent folder structures, naming conventions, version control methods, and other metadata applied logically according to a file plan.

Table 1 (p. 4) lists the usual "big bucket" categories of information that every planning organization manages. Each of these distinct data types should be stored in a coherent, straightforward, and consistent manner, using a **file plan** that makes sense for your needs, as described in the sidebar on data management practices on p. 5. The file plan begins with the folder structure highlighted earlier. From there, all data is sorted into appropriate folders.

Next is the separation of general and sensitive data. The file plan should acknowledge that some data will have two copies—a redacted and unredacted version. The redacted version will have sensitive information hidden from view; this version will be kept in the general categories provided in the table below. The unredacted version will be kept in the sensitive category.

The folder structure will contain information that spans many categories provided below. For example, each case within the Permit Cases folder will have general and sensitive client data, general and sensitive correspondence, and geospatial, land use, permit, and historical resource data. Each category may require different practices for use and storage.

Standards and Practices

Once the core principles are established and the department's data types are inventoried, the next step is to create standards and practices for each data category. Every category of data listed in Table 1 (p. 4) will have different requirements. The framework should define the standards for each category and then connect practices and protocols to ensure coherence at all levels with the overarching goal. This requires a careful review of each category to address the following topics:

- The main purpose of this data
- The location where this data will be stored within the folder structure
- The frequency with which the information will be used
- The accessibility of the data, or who will and will not be allowed to access it
- The frequency with which the data will be modified or updated
- The methods for modifying the data and who will be allowed to do so
- The retention period for the data

Addressing these topics will guide the development of practices and standards for the data governance plan.

Creating the Data Governance Program Team

Creating a data governance program takes time and requires the participation of the entire planning team. Planners don't need to build it alone; we can draw on best practices for defining, structuring, and managing data in collaboration with other departments and subject matter experts in our organization.

Roles and Responsibilities

All planning department staff have roles to play in the data governance program. The effort should be led by a chief data officer, guided by a data governance committee, and carried out by data stewards and users. Be sure to establish which team members hold each position or role so that all staff understand their responsibilities.

Chief data officer (CDO). The CDO is the project manager for the effort. At the organizational level, this position likely resides within the IT department. For departmental efforts, this position should be held by a senior staff member who engages with all aspects of data and has deep familiarity with each category. The CDO's responsibilities include the following:

- Recommending and implementing data management strategies and policies
- Facilitating committee and team meetings on the topic
- Overseeing data governance and data quality initiatives
- Coordinating data-related activities across different departments
- Ensuring compliance with data protection and privacy regulations
- Promoting data-driven decision-making and data literacy within the organization
- Monitoring and auditing performance
- Reporting results and recommended actions to the data governance committee and the broader management team

Data governance committee. The data governance committee establishes the department's data governance policy structure and advises, oversees, and monitors the data governance effort. Ideally, these committees are formed at the organizational level and represent all departments, but establishing a committee for the planning department's effort is vital. The committee should comprise five to eight members and include planning staff of different levels and roles, as well as representatives from key partner departments such as IT and legal. The committee is responsible for the following actions:

- Establishing the goal statement and principles of the data governance policy
- Overseeing an inventory of the department's data: what data is being collected, how it is stored, what is its quality, and how it is used
- Overseeing the development of data governance standards and practices
- Determining responsibility for ownership and stewardship of different types of data
- Establishing a regular system of reviewing and addressing issues of data quality and continuous improvement
- Resolving data-related conflicts and issues
- Providing feedback and guidance to the broader team

Data stewards. Data stewards have direct oversight of and immediate effect on the department's information. While the CDO and data governance committee set the direction, policies, and practices, the stewards are the ones who bring such things to fruition. Managing their workload is essential;

expectations and timeframes for implementing changes in data management practices must be compatible with their broader job responsibilities. Data stewards will often discover issues when implementing data governance practices. They should take these to the CDO, who should consider those concerns thoroughly and bring them to the committee to address. Data stewards carry out the following tasks:

- Overseeing and managing specific data sets or data domains
- Ensuring data quality, accuracy, and integrity
- Defining data standards and data definitions
- Identifying the gaps in training and education on data management practices
- Promoting data literacy and data-driven decision-making across the organization
-

Data users. All department members are data users and are therefore participants in the data governance project. When their interactions with data comply with policy, it makes everyone's job easier and the governance project successful. An effective CDO will make sure that every user feels like they are a critical piece in the puzzle with consistent guidance and support for the following tasks:

- Following data management policies and guidelines
- Using data responsibly and ethically for authorized purposes
- Reporting data-related issues and anomalies to data stewards or administrators

Working With the IT Department

Your colleagues in the IT department will be essential to the success of any data governance strategy. If they are not already directing such an effort, they will likely be happy to help you start this project. After all, IT wants everyone to value data as much as they do, and governance is the best way to do so.

Begin by sharing your initial framework with IT prior to engaging your staff or other partners and ask them what approaches are optimal, feasible, and practical based on local context and constraints. Keep in mind that IT staff are busy; something as demanding and nuanced as a governance project will require time that might not be immediately available. If the IT department already has a data governance approach, any department-specific effort should be an extension of and embedded within existing practice. Stay in regular communication with IT. The ultimate goal is to achieve the outcomes of a data governance practice with secure, structured data that has all the qualities and conditions described in this *Memo*. Your IT colleagues will be your primary partners in getting you there.

Rebuilding Better in Albemarle, North Carolina

In early 2023, the City of Albemarle, North Carolina, suffered a catastrophic network issue that led to a loss of all data stored on its networks. For the planning department, this meant a total loss of all digital files related to permitting, GIS data, reports, spreadsheets, archives, and more.

This was a huge setback for the planning team. These losses came at a time of record development activity. Also, the city was on the cusp of beginning a comprehensive planning effort that would have leveraged much of the information that was lost.

Yet there was opportunity to be found in the hardship. The department had spent years trying to restructure its data on the network and deploy better management practices, but with so many other issues to address, this never became a top priority. The crisis was a chance to bring focus to this long-standing need.

Retrofitting the existing system was difficult and time-consuming because data had to be recovered, remapped, and often repurposed. Legacy systems also posed a barrier; the department's older permitting software wasn't cloud-based and didn't capture all workflows, and migrating and integrating planning data into a better system with new software was a tremendous amount of work.

But for Albemarle, it brought data governance into the spotlight. The team is not only building a new, better approach for all the practices highlighted in this article, from file structures to naming conventions to team roles for stewardship, it is also installing new systems that synergize the inputs, workflows, and outputs in a way that is more secure, reliable, and eventually more robust than what they had before. Starting with a clean slate has led to more options and urgency. Structuring the data with the principles found in the sidebar on p. 5 gives them the opportunity to leverage the information more effectively in the new system.

According to Albemarle's planning director, Kevin Robinson, AICP, the key was to stay positive. The catastrophe offered an opportunity to redesign the department's data resources in a way that improved operations and implement policies and rules to prevent the issues that plagued the old system. Making the case for rebuilding or retrofitting data management structures is also critical when undertaking this demanding task: it is important that elected officials and stakeholders understand what you are doing, how much work it requires, and how much value they will all see at the end of it. Finally, Robinson emphasized the importance of the chief data officer role as described in this *Memo*. Effectively maintaining a data management practice requires someone charged with that responsibility in a dedicated role.

Albemarle's sudden loss of data was unfortunate. But the planning department has rebuilt their system better than it was before. By formalizing governance projects with the guidance provided in this *Memo*, and instituting best practices wherever possible, planners can make real improvements before a crisis hits.

Action Steps for Planners

The best time to begin a data governance program is now. Here are key steps to begin moving your data governance initiative forward.

Step 1: Identify and schedule meetings with key partners. Select your likely partners and participants who will help you build the department's policy framework. This includes representatives from IT, procurement, and legal, along with planning staff who have the interest and expertise to help as committee members and stewards. Share this *Memo* and notable examples from the resources highlighted in the sidebar below. Start a conversation about what is most important and feasible.

Step 2: Designate key roles. Your effort will rely on staff involvement. Select representatives to serve on the data governance committee. Identify the staff who already serve in informal data steward roles. Every team will have a few members who are enthusiastic about this work. Find and recruit these people so that they can be there at the start.

Step 3: Begin the data inventory and assessment process. The development and implementation of a data governance strategy will take some time. Meanwhile, begin the parallel process of cataloging your data from each category

Resources for Data Governance Best Practices

Much has been written about the importance of establishing an organizational data governance policy and the key components of these programs. Helpful resources to bolster your understanding of the project ahead include the following:

- What Is Data Governance? (Microsoft). This website provides a useful overview of the purpose and benefits of data governance in the context of Microsoft's Cloud services, a common industry provider for local government.
- What Is Data Governance? (Google). This website provides a useful overview in the context of Google's Cloud Services, a common industry provider for local government.
- *Model Data Governance Policy and Practice Guide for Cities and Counties* (Metrolab Network). This guide takes the principles and concepts established by the examples from Microsoft and Google and translates them to the local government context.
- *Data Inventory Guide* (Johns Hopkins University and the Bloomberg Center for Government Excellence). This guide is designed to help cities understand and carry out data inventories; the GovEx Lab website provides a comprehensive set of resources for the entire municipal data governance process.
- *Data Governance Checklist* (Florida Department of Transportation). This is an excellent example of a data audit checklist. The key questions in each category can be applied to most practices.
- *Electronic Records Policy Toolkit* (Municipal Resource and Services Center). This toolkit based on Washington State data retention policies provides excellent guidance for creating local policies for electronic record retention.

Many major municipal governments and federal agencies have already undertaken this work, and planners can look to these examples to inform the development of their own core principles and policies:

- United States Department of Transportation Federal Highway Administration's *Data Governance Primer*. This is an excellent example of how to develop clear, meaningful standards and practices for an agency's data.
- Charleston, South Carolina's *Open Data Policy*. This data governance strategy is established by an ordinance adopted by City Council and embedded within the broader context of a commitment to transparency and open data.
- Dallas's *Data Governance Standard* and *Data Management Strategy 2019–2022*. This data governance standard defines the city's data governance mission, purpose, scope, goals and objectives, and guiding principles, and it establishes data positions and committee stakeholders for the data governance effort. The data management strategy is illustrated in a process flow chart.
- Portland, Oregon's Smart City PDX *Data Privacy and Information Protection Principles*. This thorough, thoughtful mission statement brings forward meaningful objectives that can be measured and monitored over time.
- New York City's *Data Quality Standards and Review Process*. This document provides a series of self-assessment checklists for data sets that can ensure all data is provided in a consistent format that meets departmental standards for quality.
- San Francisco's *Data Management Policy*. This document establishes required data management policy for all city departments and offers a very cohesive, intuitive approach to governing data that focuses on dataset identification and classification, data sharing processes and policies, and interdepartmental data standards.
- Seattle's *Privacy Principles*. This document informs the public about how the city collects, uses, discloses, and retains personal information. Sharing this information enhances transparency and helps build trust with residents about data collection and management.
- Burlington, Vermont's *Data Strategy and Governance*. This policy establishes open data provision as a service to the community in line with the city's equity and accessibility policies while addressing issues of privacy and collection of personal data.

listed in Table 1. Gauge the quality and integrity of the data you currently hold. Map out the current structure—however confusing it might be—and start looking for the data gaps and inconsistencies. This is one of the most challenging tasks the team will face; the sooner it starts, the better. The final inventory will create the foundation for effective data management. The City of Chattanooga, Tennessee, offers helpful data inventory guidance; see also the resources in the sidebar on p. 8.

Step 4: Create your filing plan. Using the example in the sidebar on p. 5, develop a new folder structure for your data. Establish naming conventions and version control methods for the files in the new hierarchy. Document the logic and rationale for how the data will be managed. This will become the foundation for your governance policies.

Step 4: Establish your data governance policy. Assemble your data governance committee and establish the goals and core principles of your policy. (See the examples provided in the sidebar on p. 8.) Next, begin the process of reviewing your data inventory and current structure. Compare it to your filing plan. Review each category of information and determine how that information should be stored, secured, retained, and used. Document these standards and practices to establish consistent approaches.

Step 5: Implement the plan. Once the committee has assessed the inventory, developed the filing plan, and established the policies, it is time for implementation. Create the new folder structure, rename files, and move them to the appropriate locations on the shared network drive. Issue new access and usage rights and data validation procedures. Train staff on the new policies and practices and answer all questions along the way.

Step 6: Continue to evaluate and improve your data management practices. Once implementation is complete, data stewards should regularly monitor data practices and conditions and report any issues to the CDO or governance committee. Issues will often emerge and the CDO, stewards, and committee will need to adjust policies and practices as necessary to keep the information well organized and used.

This is also where a regular auditing practice monitored and managed by the data stewards will come into play. Every month or so, take a moment to look at the system as a whole and find any weaknesses that can be managed proactively. Every six months, perform the audit fully to report the status of your ongoing efforts. Use a checklist, such as the data governance checklists provided by the Florida Department of Transportation or the National Center for Education Statistics. These examples are tailored to their agencies and take slightly different approaches, but can give you a strong start in developing your own checklist.

Conclusion

The data landscape of today's planning offices is flooded with unmet needs, potential improvements, and serious liabilities. Data governance is a critical approach to tap the potential of our vast oceans of information for the betterment of our communities while balancing transparency and privacy rights through ethical, responsible data practices. This *PAS Memo* introduces the framework, concepts, and best practices for transforming data into a viable resource for planning practice.

Though it requires time and effort to transform a department's information into a more cohesive, effective structure, the benefits are many. For staff, a better data management practice will lead to more convenient access, higher-quality information, and better decision-making. For the public, holistic governance policies—especially around sensitive information and ethical data use—will provide better protection and deeper trust in our services.

Data has already improved the practice of planning, but there are many more ways that we can protect our residents, strengthen our analyses, bolster our capabilities, and increase the value that we deliver to the community. As systems thinkers and multidisciplinary practitioners, planners can use data governance as the foundation of our work. Data is a resource to be developed and managed responsibly, like the city itself. By bringing multiple perspectives into the effort, and leading with our ethical obligations at the start, data governance is another way in which planners can show how versatile and enterprising our profession can be.

About the Author

Norman Wright, AICP, is the founder of Parameter, a design and analytics consultancy that specializes in creating plans, policies, and best practices for local governments. Prior to this, he was a local government executive leading planning, economic development, and community development efforts in Oregon, Colorado, Tennessee, and South Carolina. His teams have delivered award-winning work recognized by the American Planning Association and Urban Land Institute. He holds a master's degree in city and regional planning from Clemson University.

Acknowledgment

The author would like to thank Kevin Robinson, AICP, and Krishna Namburi for providing case study information and insights that enriched this report.

PAS Memo *124 | June 2025*. PAS Memo *is a publication of APA's Planning Advisory Service. Joel Albizo, FASAE, CAE, Chief Executive Officer; Petra Hurtado, PhD, Chief Knowledge & Foresight Officer; Ann F. Dillemuth, AICP, PAS Editor. Learn more at planning.org/pas.*

 PAS Memo *(ISSN 2169-1908) is published by the American Planning Association, 200 E. Randolph Street, Suite 6900, Chicago, IL 60601; planning.org.*