CHESTERFIELD COUNTY
ADMINISTRATIVE POLICIES AND PROCEDURES

Department:	**Information Systems Technology**	**Policy Number:**	**7-xx**
Subject:	**Open Data Policy**	**Supersedes:**	
		Date Issued:	**05/26/17**

I. INTRODUCTION

All data generated by the government must be made available to the public in open, machine-readable formats. An Open Data Policy ensures that county departments manage county information as an asset.

A. Purpose

Open data is powering a new civic movement that is changing the way citizens experience our nation's cities, counties, and states. The Chesterfield County Open Data Policy is designed to make county desirable high value data more accessible to entrepreneurs, researchers and the public in general with the intent of increasing economic opportunities and growth. As IST modernizes county systems, efforts will be made to make this data "machine-readable" in order to become more transparent, participatory and collaborative.

This process will be implemented in a manner committed to protecting privacy, confidentiality and security. IST will make open data the default policy of the county instead of discretionary. IST will build a Data Catalog (an index of our data), produce a public list of our public data, and maintain a list of all data that can be made public.

B. Scope

This policy applies to all new information collection, creation, and system development efforts as well as major modernization projects that update or re-design existing information systems. These policy requirements apply to management of all "datasets" used in department information systems. Departments are encouraged to improve the discoverability and usability of existing datasets by making them "open" using the methods outlined in this policy, and prioritizing those that have already been released to the public or otherwise deemed high-value or high-demand through engagement with customers.

Departments should exercise judgment before publicly distributing data residing in an existing system by weighing the value of openness against the cost of making that data public.

II. POLICY STATEMENT

It is the policy of the Chesterfield County to practice Open Government, favoring participation, transparency, collaboration and engagement with the people of Chesterfield County and its stakeholders.

Information technologies, including web-based and other Internet applications and services, are an essential means for Open Government. Chesterfield County will continue to expand and deepen the County's innovative use of information technology toward the end of Open Government, including development and use of mobile computing and applications, provision of online data, services and transactions.

Chesterfield County also has an obligation to secure protected data based upon privacy, sensitivity, confidentiality laws or other requirements that protected data not be released in violation of applicable those laws.

III. RESPONSIBILITIES

A. Department Heads and Constitutional Officers

Department heads must ensure that staff understands how to identify information that may require additional protection and county business process activities that may require additional safeguards.

B. Chief Information Officer (CIO)

The CIO is assigned responsibility for promoting the effective and efficient design and operation of all major system processes within the county. Accordingly, The CIO ensures that technology managers positioned with the responsibility and authority to implement the requirements of this policy coordinate with County Attorney, Public Affairs, open government staff, web manager or digital strategist, program owners and other leadership, as applicable.

The CIO will also provide leadership to help departments improve the interoperability and openness of government information. To this end, the CIO will work to establish an enterprise working group. The working group should focus on leveraging government-wide communities of practice to help with the development of tools that support information interoperability and openness through open repositories. Part of this work should be to share best practices related to interoperability and openness within government (e.g., Federal, state, local, and tribal). These collaborations shall be subject to statutory limitations and conducted in a way that fully protects privacy, confidentiality, confidential business information, and intellectual property rights.

C. Information Security Manager

A key component of departments' management of information resources involves working closely with information security and other relevant officials to ensure that each stage of the planning process includes a full analysis of privacy, confidentiality, and security issues.

IV. Technical & Policy Controls

A. Chesterfield County recognizes Open Government as a key means for enabling public participation, transparency, collaboration and effective government, including by ensuring the availability and use of Open Data, appropriate security and sharing of Protected Data, effective use of Identity and Access Management and engagement of stakeholders and experts toward the achievement of Open Government.

B. Chesterfield County Chief Information Officer ("CIO"), in consultation with County departments, is authorized and directed to issue a Chesterfield County Open Data Policy.

C. The Open Data Policy shall include standards for the format and publishing of such data and guidance on accessibility, re-use and minimum documentation for such data.

D. The Open Data Policy shall include guidance for departments on the classification of their data sets as public or protected and a method to report such classification to the CIO. All departments shall publish their public record data sets on the Chesterfield County open data portal to the extent such data sets are determined to be appropriate for public disclosure, and/or if appropriate, may publish their public record data set through other methods, in accordance with API, format, accessibility and other guidance of the Open Data Policy.

E. The Chesterfield County CIO, in consultation with County departments, is authorized and directed to issue a Chesterfield County Protected Data Policy applicable to non-public data, such as health data, educational records and other protected data.

F. The policy shall provide guidance on the management of Protected Data, including guidance on security and other controls to safeguard Protected Data, including appropriate Identity and Access Management and good practice guidelines for compliance with legal or other rules requiring the sharing of Protected Data with authorized parties upon the grant of consent, by operation of law or when otherwise so required.

G. The policy shall provide a method to ensure approval by County Attorney to confirm Protected Data is only disclosed in accordance with the Policy.

H. This policy is not intended to diminish or alter the rights or obligations afforded under applicable laws. Additionally, this policy is intended to be interpreted consistent with Federal, Commonwealth, and local laws and regulations regarding the privacy, confidentiality, and security of data. Nothing herein shall authorize the disclosure of data that is confidential, private, exempt or otherwise legally protected unless such disclosure is authorized by law and approved by the County Attorney of Chesterfield County.

I. This policy is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against Chesterfield County, its departments, departments, or entities, its board members, officers, employees, or agents, or any other person.

J. The Chesterfield County CIO is authorized and directed to regularly consult with experts, thought leaders and key stakeholders for the purpose of exploring options for the implementation of policies and practices arising under or related to this policy.

V. Definitions

Public Information

All datasets accessed published as public information must not contain National Security information as defined by statute and/or Executive Order, or other information/data that is protected by other statute,

practice, or legal precedent. The supplying Department is required to maintain currency with public disclosure requirements.

Security

All information accessed through published as public information will be in compliance with the required confidentiality, integrity, and availability controls mandated by law or as best practices identified by the National Institute of Standards and Technology (NIST).

Privacy

All information accessed published as public information must be in compliance with current privacy requirements. In particular, departments are responsible for ensuring that the datasets published as public information address privacy concerns.

Data Quality and Retention

All information published as public information is subject to the Information Quality Act (P.L. 106-554). For all data accessed published as public information, each department will confirm that the data being provided through this site meets the county's Information Quality Guidelines.

As the authoritative source of the information, submitting Departments are responsible for ensuring that the datasets accessed published as public information are current and correct, in compliance with record retention requirements outlined by the governing retention and archives authority, Library of Virginia.

Secondary Use

Data published as public information does not, and should not; include controls over its end use. Once the data has been downloaded from the county's site, the government cannot vouch for their quality and timeliness. Furthermore, the county cannot vouch for any analyses conducted with data retrieved from the data published as public information.

Attribution

While not required, when using content, data, documentation, code, and related materials published as public information in your own work, we ask that proper credit be given. An example citation is provided below:

Data retrieved from information published as public information (https://www.chesterfield.gov/open)

Disclaimer of Endorsement

The information posted on the *https://www.chesterfield.gov/open* website includes hypertext links, or pointers, to information created and maintained by other public and/or private organizations. It only provides these links and pointers for information and convenience. When a link is selected to an outside website, the site visitor will be informed that they are leaving the open gov site and are subject to the privacy and security policies of the owners/sponsors of the outside website. Sample disclaimer statements are below;

- Chesterfield County does not control or guarantee the accuracy, relevance, timeliness, or completeness of information contained on a linked website.

- Chesterfield County does not endorse the organizations sponsoring linked websites and we do not endorse the views they express or the products/services they offer.

- Chesterfield County cannot authorize the use of copyrighted materials contained in linked websites. Users must request such authorization from the sponsor of the linked website.

- Chesterfield County is not responsible for transmissions users receive from linked websites.

- Chesterfield County does not guarantee that outside websites comply with Section 508 (accessibility requirements) of the Rehabilitation Act.

Public Participation

In support of county Transparency and Open Government initiatives, recommendations from individuals, groups and organizations regarding the presentation of data, data types, and metadata will contribute to the evolution of Chesterfield County open government.

Data

For the purposes of this policy, the term "data" refers to all structured information, unless otherwise noted.

Dataset

For the purposes of this policy, the term "dataset" refers to a collection of data presented in tabular or non-tabular form.

Government information

"Government information" in the context of this policy means information created, collected, processed, disseminated, or disposed of, by or for Chesterfield County.

Information

"Information" means any communication or representation of knowledge such as facts, data, or opinions in any medium or format, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

Information life cycle:

The term "information life cycle" means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

Personally identifiable information

"Personally identifiable information" (PII) refers to information that can be used to distinguish or trace an individual' s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. It is important for a county department to recognize

that non-PII can become PII whenever additional information is made publicly available (in any medium and from any source) that, when combined with other available information, could be used to identify an individual.

Mosaic effect

The mosaic effect occurs when the information in an individual dataset, in isolation, may not pose a risk of identifying an individual (or threatening some other important interest such as security), but when combined with other available information, could pose such risk. Before disclosing potential PII or other potentially sensitive information, departments must consider other publicly available data –in any medium and from any source-to determine whether some combination of existing data and the data intended to be' publicly released could allow for the identification of an individual or pose another security concern.

Open data

For the purposes of this policy, the term "open data" refers to publicly available data structured in a way that enables the data to be fully discoverable and usable by end users. In general, open data will be consistent with the following principles:

- *Public* – Departments must adopt a presumption in favor of openness to the extent permitted by law and subject to privacy, confidentiality, security, or other valid restrictions.

- *Accessible* - Open data is made available in convenient, modifiable, and open formats that can be retrieved, downloaded, indexed, and searched. Formats should be machine-readable (i.e., data are reasonably structured to allow automated processing). Open data structures do not discriminate against any person or group of persons and should be made available to the widest range of users for the widest range of purposes, often by providing the data in multiple formats for consumption. To the extent permitted by law, these formats should be non-proprietary, publicly available, and no restrictions should be placed upon their use.

- *Described* - Open data is described fully so that consumers of the data have sufficient information to understand the data's strengths, weaknesses, analytical limitations, security requirements, as well as how to process them. This involves the use of robust, granular metadata (i.e., fields or elements that describe data), thorough documentation of data elements, data dictionaries, and, if applicable, additional descriptions of the purpose of the collection, the population of interest, the characteristics of the sample, and the method of data collection.

- *Reusable* - Open data is made available under an open license that places no restrictions on their use.
- *Complete* - Open data is published in primary forms (i.e., as collected at the source), with the finest possible level of granularity that is practicable and permitted by law and other requirements. Derived or aggregate open data should also be published but must reference the primary data.

- *Timely* - Open data are made available as quickly as necessary to preserve the value of the data. Frequency of release should account for key audiences and downstream needs.

- *Managed Post-Release* - A point of contact must be designated to assist with data use and to respond to complaints about adherence to these open data requirements.