



**KING COUNTY**

1200 King County Courthouse  
516 Third Avenue  
Seattle, WA 98104

**Signature Report**

**December 6, 2016**

**Motion 14760**

**Proposed No. 2016-0228.1**

**Sponsors Upthegrove**

1           A MOTION approving a report regarding protecting county  
2           constituent personal information upon implementation of  
3           the county's constituent engagement service , as required by  
4           the 2015/2016 Biennial Budget Ordinance, Ordinance  
5           17941, Section 129, as amended by Ordinance 18189,  
6           Section 6, Proviso P12.

7           WHEREAS, Ordinance 18189, Section 6, Proviso P12, which was an amendment  
8           to the 2015/2016 Biennial Budget Ordinance, Ordinance 17941, Section 129, as  
9           amended, was passed by council on December 16, 2015, and

10           WHEREAS, the ordinance states, "Of the appropriation for capital project  
11           1121493, constituent engagement services, \$100,000 shall not be expended or  
12           encumbered until policies for protecting constituents' personal information are adopted  
13           and published and the council passes a motion approving a report outlining how  
14           constituent's personal information will be protected. The motion shall reference the  
15           subject matter, the proviso's ordinance, ordinance section and proviso number in both the  
16           title and body of the motion";

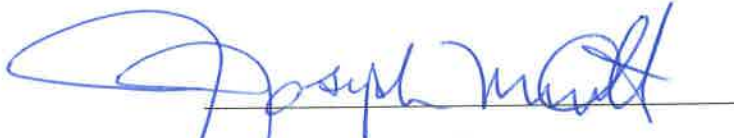
17           NOW, THEREFORE, BE IT MOVED by the Council of King County:

18           The report entitled Personal Information and Privacy within King County  
19 Government - Response to King County Ordinance 18189, Section 6, Proviso P12, which  
20 is Attachment A to this motion, is hereby approved.  
21

Motion 14760 was introduced on 4/25/2016 and passed by the Metropolitan King  
County Council on 12/5/2016, by the following vote:


Yes: 8 - Mr. von Reichbauer, Ms. Lambert, Mr. Dunn, Mr.  
McDermott, Mr. Dembowski, Mr. Upthegrove, Ms. Kohl-Welles and  
Ms. Balducci  
No: 0  
Excused: 1 - Mr. Gossett

KING COUNTY COUNCIL  
KING COUNTY, WASHINGTON



J. Joseph McDermott, Chair

ATTEST:



Melani Pedroza, Acting Clerk of the Council

**Attachments:** A. Personal Information and Privacy within King County Government



# Personal Information and Privacy within King County Government

Ralph Johnson  
Chief Information Security and Privacy Officer





# Personal Information and Privacy within King County Government

## Contents

- Introduction ..... 1
- Background ..... 1
  - Personal Information ..... 1
    - What Constitutes Personally Identifiable Information (PII)..... 1
  - Privacy ..... 2
    - Definition ..... 3
    - Privacy Principles ..... 3
  - Rights and Responsibilities Relating to Protecting Information ..... 4
    - Legal Obligation to Protect Personally Identifiable Information ..... 5
- How King County Protects Personally Identifiable Information ..... 6
  - King County Code..... 6
  - King County’s Information Privacy Policy and Privacy Notice ..... 7
  - Privacy and Personally Identifiable Information and Public Disclosure ..... 9
- Recommended Improvements to Address Personally Identifiable Information and Privacy ..... 10
  - Policy Improvements ..... 10
    - Examine and Update Current King County Code ..... 10
    - Review and Enhance King County’s Privacy Policy ..... 12
    - Codify aspects of the Privacy Policy ..... 12
  - Operational Improvements..... 13
    - Publish a Privacy Guide ..... 13
    - Ensure that all King County Workforce Members are Educated on the Concept of Privacy and Personally Identifiable Information ..... 13
    - Inventory Personally Identifiable Information Using a Privacy Impact Assessment (PIA)..... 13
- Personally Identifiable Information and Privacy in the Constituent Relationship Management System (CRM) ..... 14
- Conclusion ..... 15



## Introduction

King County Council passed ordinance 18110 that included the following proviso related to Constituent Engagement Services project:

*P12 PROVIDED FURTHER THAT:*

*“Of the appropriation for capital project 1121493, constituent engagement services, \$100,000 shall not be expended or encumbered until policies for protecting constituents’ personal information are adopted and published and the council passes a motion approving a report outlining how constituent’s personal information will be protected. The motion shall reference the subject matter, the proviso’s ordinance, ordinance section and proviso number in both the title and body of the motion.”*

This report outlines how is the constituent’s personal information is protected under the current privacy policy and privacy notice, provides information on how King County respects and manages personal information of residents and others with whom King County interacts, and provides recommendations on improving the County’s existing policies and practices for protecting personal information.

## Background

### Personal Information

This concept is more commonly referred to as “Personally Identifiable Information” (PII). The National Institute of Standards and Technology (NIST) in their Special Publication 800-122 entitled **Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)**<sup>1</sup> provides the following definition for PII:

*“any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information..”*

### What Constitutes Personally Identifiable Information (PII)

To become “Personally Identifiable Information” distinct data points about an individual must be combined. Data is simply a piece of information. For example, let’s start with the smallest piece of data that can be interpreted by a human and that is a letter of the alphabet. If we have a “B”, this tells us nothing, combine it with an “r” and we still have nothing. Add in an “own” and we have Brown. This could be a last name or a color so we are beginning to get something that has meaning, this is information. At this point though we don’t have much information and definitely nothing identifiable. If we add in “Joe”, now we begin to have identifiable information but there are probably millions of Joe Brown’s, therefore it is not yet personally identifiable. Then we add in an address; we get more identifiable, but there could be a father and son living at that address with the same name. Now add in a Social Security Number or Driver’s License and now we have identified a specific individual. This is how

<sup>1</sup> NIST Special Publication 800-122 **Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)** – <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>

data points become “Personally Identifiable Information” or PII. As stated in the above definition, PII usually consists of, but may not be limited to, combinations of the following:

#### *Personal Information*

- Name (First, First Initial, Middle, Middle Initial and Last)
- Gender
- Date of Birth
- Home Address (Health Insurance Portability and Accountability Act uses “any geographical designation smaller than a State”)
- Personal Telephone Number
- Personal e-mail address
- Personal IP (internet protocol) address
- Employee Identification Number
- Employment History
- Biometric identifiers
- Photograph or video identifiable to an individual
- Government Issued Identifiers (Social Security, Driver’s License, State ID, Passport, License Plate Numbers)
- Genetic Information
- Behavioral Information

#### *Medical Information*

- Medical Records
- Health Plan/Beneficiary information
- Insurance ID Numbers
- Physical or Mental Health Information
- Provided Health Services or any information collected during the health service

#### *Financial Information*

- Account Numbers (credit cards, bank accounts, etc.)
- Personal Identification Numbers (PIN) for account numbers
- Credit History Information

#### *Sensitive Information*

- Racial or ethnic origin
- Religious or philosophical beliefs
- Trade union memberships
- Health and sexual orientation
- Offenses, criminal convictions or security measures
- Personnel related information

King County collects and protects this information as part of providing services across its many lines of business.

#### Privacy

Privacy has many different connotations. There is the concept of physical privacy, which focusses on being left alone and not observed. However, in the context of this analysis, the focus will be on that of



“Information Privacy.” In this context, privacy is much broader than just protecting the confidentiality of Personally Identifiable Information.

#### Definition

Merriam-Webster dictionary defines “Privacy” as:

- a: the quality or state of being apart from company or observation: seclusion*
- b: freedom from unauthorized intrusion <one's right to privacy>*

The meaning of “Information Privacy” is more vague and elusive. It is important to understand information privacy is an umbrella term for a group of related yet distinct things. Information privacy is about respecting the desires of individuals, where compatible with the aims of the larger community. Information privacy is not just about what people expect, but about what they desire. Information privacy is not merely an individual right – it is an important component of any flourishing community<sup>2</sup>. To that end King County’s **Information Privacy Policy**<sup>3</sup> defines Information Privacy as:

*“Ensuring that individuals maintain the ability to control what information is collected about them, how it is used, who has used it, who maintains it and what purpose it is used for as provided within the law.”*

This definition supports the individual’s right to influence and control the use of his/her personal information and is based on the privacy principles discussed below.

#### Privacy Principles

The National Institute of Standards and Technology (NIST) Special Publication 800-122 entitled **Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)** puts it interestingly when it states:

*“...the protection of PII and the overall privacy of information are concerns both for individuals whose personal information is at stake, and for organizations that may be liable or have their reputations damaged should such PII be inappropriately accessed, used, or disclosed. Treatment of PII is distinct from other types of data because it needs to be not only protected, but also collected, maintained, and disseminated in accordance with the needs of the organization but also the law.”*

The Organization for Economic Co-operation and Development (OECD) Privacy Guidelines were developed in 1980 and are the most widely-accepted privacy principles.

The Organization for Economic Co-operation and Development (OECD) identified the following eight (8) Fair Information Practices<sup>4</sup>.

<sup>2</sup> Paraphrased from Cornell University’s Working Definition of Privacy web page:

<http://www.it.cornell.edu/policies/infoprivacy/definition.cfm>

<sup>3</sup> King County’s Information Privacy Policy

[http://www.kingcounty.gov/~media/operations/it/governance/policies/Information\\_Privacy\\_Policy\\_Signed060910.ashx?la=en](http://www.kingcounty.gov/~media/operations/it/governance/policies/Information_Privacy_Policy_Signed060910.ashx?la=en)

<sup>4</sup> OECD Privacy Principles: <http://oecdprivacy.org/>

- **Collection Limitation** – There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data Quality**—Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
- **Purpose Specification** – The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- **Use Limitation**—Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except with the consent of the data subject or by the authority of law.
- **Security Safeguards** – Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
- **Openness** – There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
- **Individual Participation** – An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.
- **Accountability** – A data controller should be accountable for complying with measures which give effect to the principles stated above.

#### Rights and Responsibilities Relating to Protecting Information

What is a right to one party regarding the collection, use and disclosure of information represents a responsibility for another party.

King County collects a large amount of necessary information about residents and others with whom they do business. Certain pieces of data that would otherwise be considered personal, and thus confidential, are deemed public information and therefore provided to the government as a matter of course, often times not provided by the “consumer” but by a third party. One example of this is third party provision is through the filing of documents with the recorder’s office.

However King County obtains the information, residents and those engaged in interactions with King County have a right to expect that King County protect this information to the extent allowed by law, it is King County’s responsibility to ensure appropriate protection.

## Legal Obligation to Protect Personally Identifiable Information

There are a number of legal obligations in which Personally Identifiable Information has a role. These obligations include, but may not be limited to:

- Health Information Portability and Accountability Act (HIPAA) with the accompanying Health Information Technology for Economic and Clinical Health Act (HITECH)
  - HIPAA – Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996
  - HITECH – Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub.L. 111–5)
- Fair and Accurate Credit Transactions Act (FACTA) of 2003 – Federal Trade Commission (FTC) Red Flags Rules
- Children's Online Privacy Protection Act of 1998 (COPPA) 15 U.S.C. §§ 6501–6506 (Pub.L. 105–277, 112 Stat. 2681-728, enacted October 21, 1998.
- Criminal Justice Information Systems (CJIS) – Federal Bureau of Investigations (FBI) Policy
- Washington State RCWs include but may not be limited to:
  - 42.56.230 RCW Personal Information
  - 42.56.240 RCW Investigative, law enforcement, and crime victims.
  - 42.56.250 RCW Employment and licensing
  - 42.56.360 RCW Health Care
  - 42.56.380 RCW Client records of domestic violence programs, or community sexual assault programs or services for underserved populations
  - 42.56.440 RCW Veterans' discharge papers—Exceptions.
  - 42.56.590 RCW Personal information—Notice of security breaches
  - 70.02 RCW MEDICAL RECORDS—HEALTH CARE INFORMATION ACCESS AND DISCLOSURE
- Payment Card Industry (PCI) Data Security Standard (DSS)
- U.S. Office of Management and Budget Uniform Guidance requirements for 2 CFR Part 200 Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards

Some of these obligations have very specific requirements for protecting distinct pieces of data while others are very general in their description of Personally Identifiable Information.

King County should address protecting Personally Identifiable Information and privacy universally rather than focus specifically on legal obligations. This provides more consistent application of privacy practices and complete protections to Personally Identifiable Information. Specifically focusing on compliance to laws and regulations leaves gaps, increases costs and risks.

## How King County Protects Personally Identifiable Information

### King County Code

KCC 2.14.010 **Definitions**<sup>5</sup> provides a few pertinent terms related to Personal Information. These are:

*“C. “Personal data” means any information concerning an individual that, because of name, identifying number, image, mark or description, can be readily associated with a particular individual, including information contained in printouts, forms, written analyses or evaluations.*

*D. “Personal identifying data” means social security number, date of birth or mother’s maiden name.”*

KCC 2.14.030 **Commitment to Protecting Privacy** enacted in 1996 and revised in 2010 which reads as follows:

*“King County is committed to balancing the promotion of public access to information with the privacy rights of its citizens by adhering to the following guidelines:*

*A. Collection of personal data shall be lawful, fair, and to the extent possible with the knowledge and consent of the individual;*

*B. Agencies shall establish procedures to ensure that data is accurate, complete, current and relevant to the agency’s mandated functions;*

*C. When data can only be collected with the consent of the individual, the purpose for the data shall be stated upon collection. Personal data should not be used by the county for any purpose not stated upon collection without the consent of the data subject or by the positive authorization of law. This is not intended to limit collection of personal data for purposes of investigative agencies or other functions which collect non-disclosable information according to chapter 42.56 RCW or any other federal, state, local statute, rule or regulation;*

*D. Personal data shall be reasonably protected by the data collector;*

*E. Agencies shall establish mechanisms for citizens to review information about themselves and to submit corrections of possible inaccuracies in that information; and*

*F. The executive shall submit a report by October 1 of every year filed in the form of a paper original and an electronic copy to the clerk of the council, who shall retain the original and provide an electronic copy to all councilmembers and committee coordinator for the government and accountability committee or its successor. The report shall list by category new and existing personal data collected by county agencies, a description of the uses of this personal data and its public disclosure status. (Ord. 17008 § 3, 2010; Ord. 12550 § 3, 1996).”*

As stated in KCC 2.14.030 above, King County respects the privacy of its citizens. Therefore all Personally Identifiable Information relating to those engaged in interactions with King County are treated as confidential and only released through a public disclosure request after the Public Disclosure Officers or public records officers consider the sensitivity of the information being requested and the potential

<sup>5</sup> KCC Title 2 – Administration [http://www.kingcounty.gov/council/legislation/~/\\_media/Council/documents/Clerk/CodeFiles/1--KCCCode Word/05 Title 2.ashx](http://www.kingcounty.gov/council/legislation/~/_media/Council/documents/Clerk/CodeFiles/1--KCCCode Word/05 Title 2.ashx)

harm that could result with the disclosure and prevailing legal concerns surrounding the requested information.

It is also important to note that the Organization for Economic Co-operation and Development (OECD) privacy principles form the foundation for KCC 2.14.030 subsections A through E.

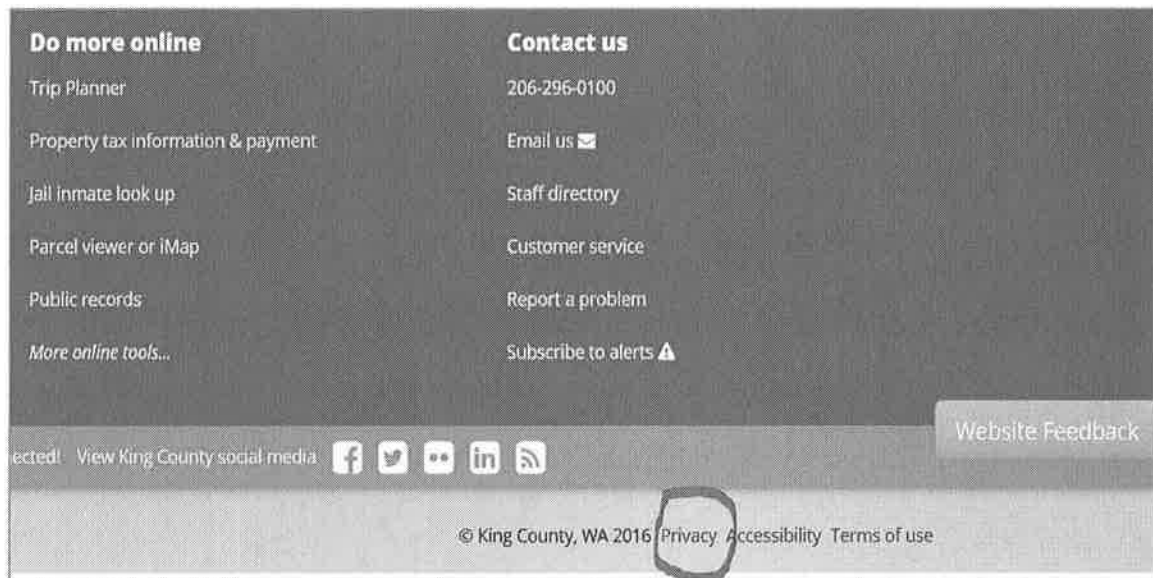
#### King County's Information Privacy Policy and Privacy Notice

King County's Information Privacy Policy<sup>6</sup> was developed in 2004 and updated in 2010 by the Office of Information Resource Management (OIRM) [now Department of Information Technology (KCIT)] through the IT Governance framework, in collaboration with all Executive branch departments and Separately Elected agencies. Accompanying this policy is a Privacy Notice<sup>7</sup> which summarizes the policy for the general public. Both the policy and notice are based on the Organization for Economic Co-operation and Development (OECD) privacy principles discussed on page 3.

The Information Privacy Policy provides a context for the management of information privacy across King County and outlines the principles that county agencies should follow. The policy also provides common definitions used to set an appropriate context.

The Privacy Notice is an easy to read document that tells residents that we receive collect and use information about them according to a set of rules.

Figure 1: King County Privacy Notice Link



All King County Web pages contain a link to this Privacy Notice as shown in Figure 1.

<sup>6</sup> King County's Information Privacy Policy can be found on the Internet at:

[http://www.kingcounty.gov/~media/operations/it/governance/policies/Information\\_Privacy\\_Policy\\_Signed060910.ashx?la=en](http://www.kingcounty.gov/~media/operations/it/governance/policies/Information_Privacy_Policy_Signed060910.ashx?la=en)

<sup>7</sup> The Privacy Notice can be found at: <http://www.kingcounty.gov/about/website/privacy.aspx>

The Privacy Notice is available in the following ten (10) languages:

- |         |            |         |          |
|---------|------------|---------|----------|
| English | Cambodian  | Chinese | Japanese |
| Korean  | Lao        | Russian | Spanish  |
| Tagalog | Vietnamese |         |          |

As with all Information Technology Governance policies, this policy is a minimum standard. Departments and/or agencies with more stringent requirements can apply more strict criteria, but not less. This leads to some departments and/or agencies having somewhat different Privacy Policies and/or Privacy Notices. For example the Department of Public Health’s Privacy Policy is based on the King County documents. However, Health Information Portability and Accountability Act (HIPAA) has certain specific requirements that proved too restrictive for King County’s overall needs. The Department of Public Health does not post their Privacy Policy<sup>8</sup> on the Internet but provides it upon request by a customer. The policy is, however available, on King County’s intranet.

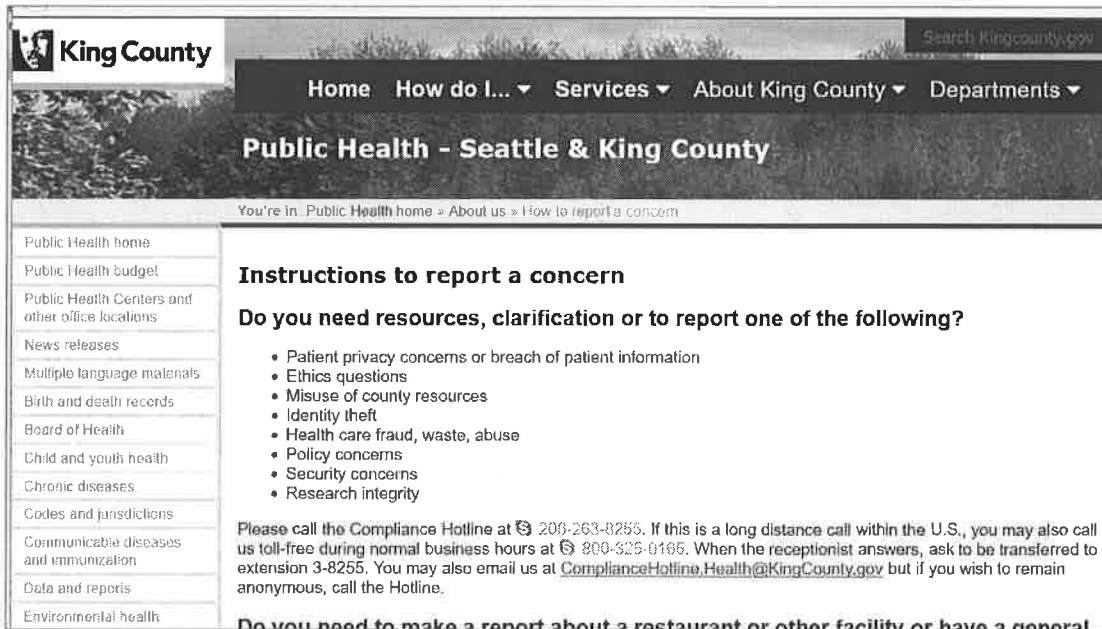
Figure 2: Department of Public Health Contact Link



Department of Public Health also provides a different contact point for concern or issue. This information is provided as a link from the department’s web page on the left banner as shown in the Figure 2 to the right.

This link provides a number of contact methods as can be seen in Figure 3.

Figure 3: Department of Public Health HIPAA Compliance Contact



<sup>8</sup> King County Department of Public Health Privacy Policy  
<https://kc1.sharepoint.com/sites/DPH/Admin/compliance/Policies/Forms/AllItems.aspx?RootFolder=%2fsites%2fDPH%2fAdmin%2fcompliance%2fPolicies%2fPHL1-2-1Privacy&FolderCTID=0x012000D6BAF4C74C5C2C4EAB1F3C1B46641739>

## Privacy and Personally Identifiable Information and Public Disclosure

The Purpose section of the King County Privacy Policy states:

*“King County, as a government entity, conducts public business. As such, the records related to the business of King County are available for public review unless an exemption applies. Nevertheless, King County is committed, to the extent allowable by law, to protect and secure personally identifiable information contained in Organization records. The privacy commitment must be balanced with the rights of public access under Chapter 42.56 RCW. (Public Records Act) and consistent with KCC 2.14.030 and any other applicable federal, state, and local statute or regulation.”*

42.56.230 RCW **Personal Information**<sup>9</sup> has clear exclusions for the release of personal information. This provision allows for the protection of personal information within many types of records such as:

- Childcare and Educational Records
- Employee, Appointed and Elected Officials Records within public agencies
- Credit card and other financial information
- Any record used to prove identity, age, residential address, social security number, or other personal information required to apply for a driver's license or identicaid
- Voluntarily submitted information contained in a database that is part of or associated with enhanced 911 emergency communications systems, or information contained or used in emergency notification systems

42.56.210 RCW **Certain personal and other records exempt**<sup>10</sup> states:

*“(1) Except for information described in \*RCW 42.56.230(3)(a) and confidential income data exempted from public inspection pursuant to RCW 84.40.020, the exemptions of this chapter are inapplicable to the extent that information, the disclosure of which would violate personal privacy or vital governmental interests, can be deleted from the specific records sought. No exemption may be construed to permit the nondisclosure of statistical information not descriptive of any readily identifiable person or persons.*

*(2) Inspection or copying of any specific records exempt under the provisions of this chapter may be permitted if the superior court in the county in which the record is maintained finds, after a hearing with notice thereof to every person in interest and the agency, that the exemption of such records is clearly unnecessary to protect any individual's right of privacy or any vital governmental function.*

*(3) Agency responses refusing, in whole or in part, inspection of any public record shall include a statement of the specific exemption authorizing the withholding of the record (or part) and a brief explanation of how the exemption applies to the record withheld.”*

<sup>9</sup> 42.56.230 RCW **Personal Information** <http://app.leg.wa.gov/RCW/default.aspx?cite=42.56.230>

<sup>10</sup> 42.56.210 RCW **Certain personal and other records exempt** <http://apps.leg.wa.gov/rcw/default.aspx?cite=42.56.210>

In short, this section states that if a specific exemption does not exist in RCW or is provided by another law or regulation from a higher authority, a public entity in Washington may be required under 42.56 RCW to release such personally identifiable information.

With this in mind, any recording of personally identifiable information relating to a resident or other entity engaged in interactions with King County may result in the disclosure of related information unless excluded in 42.56 RCW or other prevailing law.

Some personal information deemed in the public interest has been made available through the Internet and thus does not require a public disclosure request. This is for convenience of residents and businesses to facilitate conducting certain types of business with King County. Examples of such information include:

- Many, but not all, types of documents filed with the Recorder's Office (certain types of documents are not available through this avenue due to the sensitive nature of information contained in the record)
- Real estate and tax records
- Voter registration records

## Recommended Improvements to Address Personally Identifiable Information and Privacy

### Policy Improvements

#### Examine and Update Current King County Code

In today's highly computerized, data rich, online environment information and data are much more accessible and valuable. This makes it easier and more desirable for those with nefarious intent to obtain this data to engage in activities such as identity theft.

#### *Improve the Definition of "Personal Data" and "Personal Identifying Data"*

KCC 2.14.010 separates the concept of "Personal Data" and "Personal Identifying Data". The way in which this is done implies a separation of the concepts. This is not at all true. In fact, there is no such thing as "Personal Identifying Data". As stated on page 1, data is simply a piece of information. For example a person's first, middle and last names are data, their address is data, and their social security number is data. Combined these become personally identifiable information or PII.

Currently King County code KCC 2.14.010(D) identifies the following pieces of data as personally identifiable: **social security number, date of birth or mother's maiden name**. As can be seen in the section entitled **What Constitutes Personally Identifiable Information (PII)** on page 1 the list of data types that combined provide information that is considered personally identifiable is far more extensive than that listed in King County code.

#### Recommendation

Revise King County code replacing KCC 2.14.010 C and D with the definition provided by the National Institute of Standards and Technology in their Special Publication 800-122 entitled "**Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)**" which reads:



*“any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information..”*

Once this definition is revised, administrative procedures should be developed to ensure the confidentiality of information that meets the definition. Typically, in an organization, the Chief Information Officer would lead an effort to develop baseline procedures for identifying the location of all potential PII. For King County the recommendation is that such baseline procedures be developed by KCIT Information Assurance Service with collaboration from all departments and elected agencies through the County’s Information Technology Governance structure.

Such procedures might include but not be limited to:

- Identification of potential PII – This would include defining PII categories similar to those listed on page 1 as well as identification of the location of these data sets.
- Standardized processes to review and release PII – These procedures would encompass how PII is reviewed for potential release and security procedures for proper redaction and/or release of PII.
- Standardized controls to ensure the confidentiality of PII – This would be a set of required technological and process controls designed to ensure confidentiality of the PII. One example might include requiring encryption of laptop drives or USB storage media that contains PII.
- Requiring the use of a Privacy Impact Assessment (PIA) – A PIA is a tool that is used to assess the risks to privacy prior to the creation of any new data collection instrument. The PIA addresses all eight privacy principles and outlines how the system will uphold these principles.

It is important to note that such an undertaking is large and would require dedicated and committed resources and countywide participation, collaboration and cooperation. It needs to be championed by the County’s Leadership at the highest levels.

*Clarify “Privacy” in King County Code*

KCC 2.14.020 **Management and dissemination of electronic information** Subsection A(3) states.

*A. King County is committed to managing its public records as a countywide resource and in a manner that:*

*3. Protects individual privacy;*

And KCC 2.14.030 **Commitment to protecting privacy** reads:

*“King County is committed to balancing the promotion of public access to information with the privacy rights of its citizens by adhering to the following guidelines:*

In both of these references, the code is specifically referring to “Information Privacy”. However no definition of privacy or information privacy is provided.

### Recommendation

Provide a definition of Information Privacy in King County Code. As stated above, King County's Information Privacy Policy provides a clear definition of "Information Privacy" as:

*"Ensuring that individuals maintain the ability to control what information is collected about them, how it is used, who has used it, who maintains it and what purpose it is used for as provided within the law."*

### Review and Enhance King County's Privacy Policy

As previously mentioned the Privacy Policy was adopted in 2004 and updated in 2010. Information Technology Governance practices are to review all policies every 18 month. This policy is due for review and probable update. There have been some changes in technology and process which indicates a need for possible improve the Privacy Policy.

Specific revisions recommended are:

- Replace the current definition of Personally Identifiable Information with that provided in the National Institute of Standards and Technology Special Publication 800-122 "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"
- Reorganize the policy provisions to more clearly follow the Organization for Economic Co-operation and Development (OECD) privacy principles.
- Update references
- Update responsibilities
- Develop associated best practices for employees related to the identification of Personally Identifiable Information and its proper protection.

### Codify Aspects of the Privacy Policy

KCC 2.14.030 **Commitment to Protecting Privacy** is a beginning. Subparagraphs A through E touch on the Organization for Economic Co-operation and Development (OECD) guidelines, but the Privacy Policy goes further than these subparagraphs to encompass all eight (8) privacy principles. The County's Privacy Policy is one of many Information Technology (IT) Governance policies. IT Governance includes all branches of the County government. IT Governance reviews and recommends proposed policies for approval and signature by the Chief Information Officer. Elected branches of the County government either follow this policy, or develop their own that should meet the minimums set in the IT Governance policy. This inconsistency may create risk for the County in responding to resident concerns about how their information is handled across the County's systems and services. Furthermore, the Privacy Policy goes beyond information technology and it is the responsibility of all county's lines of business.

Codifying those parts of the Privacy Policy that are appropriate would require all separately elected agencies to follow the policy. By setting it as a baseline and allowing for differences in compliance with legal variances the codification could still allow individual agencies and departments to vary somewhat but a more "consistent" framework would apply.

## Operational Improvements

### Publish a Privacy Guide

The State of Washington has published a Privacy Guide intended to educate citizens on their privacy rights in relation to the State. This guide entitled **Privacy: A Guide to Washington Citizens**<sup>11</sup>, provides excellent guidance for citizens on protecting the privacy of their personal information in a digital environment.

King County should develop and publish a similar guide for residents but take it one step further by developing and publishing a second guide targeted to King County employees. This second guide would focus on how King County employees can protect the privacy of resident information.

### Ensure that all King County Workforce Members are Educated on the Concept of Privacy and Personally Identifiable Information

In order to ensure that the personal information about residents and others engaged in interactions with King County is properly protected all King County Workforce Member must be adequately educated on the topic of privacy, what constitutes Personally Identifiable Information, what impacts entities, including King County, can face if such information is inappropriately handled and how they should behave around such information.

The term Workforce Member is being used here due to the broad nature of individuals conducting work for King County. The term "Employee" is not sufficient to encompass all such individuals. Workforce Member is defined in King County's Privacy Policy as:

*"Employees, volunteers, and other persons whose conduct, in the performance of work for King County, is under the direct control of King County, whether or not they are paid by King County. This includes full and part time elected or appointed officials, members of boards and commissions, employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to King County."*

One piece of this education will of course be the Privacy Guide mentioned above, but there is much more to such education than simply publishing a pamphlet. All King County Workforce Members must be required to participate in such an education effort, potentially as part of on-boarding activities at the start of employment, and/or through a bi-annual training for existing employees.

### Inventory Personally Identifiable Information Using a Privacy Impact Assessment (PIA)

A Privacy Impact Assessment (PIA) is a decision tool used to identify and mitigate privacy risks that identifies:

- What Personally Identifiable Information (PII) an organization is collecting;
- Why the PII is being collected; and
- How the PII will be collected, used, accessed, shared, protected and stored.

A Privacy Impact Assessment (PIA) is intended to accomplish three goals:

- Ensure conformance with applicable legal, regulatory, and policy requirements for privacy;

<sup>11</sup> Privacy: A Guide for Washington Citizens can be found at <https://s3-us-west-2.amazonaws.com/ocio-website-files/PrivacyGuide2015.pdf>.

- Determine the risks and effects; and
- Evaluate protections and alternative processes to mitigate potential privacy risks.

A Privacy Impact Assessment (PIA) can provide the following benefits:

- Define the functions of privacy compliance for an organization.
- Identify the appropriate persons within the organization to perform those privacy compliance functions.
- Develop procedures to conduct an initial review of operations or systems.
- Create a process for continuing privacy compliance reviews.
- Define the privacy ramifications of new products, services, systems enhancements, upgrades operations, vendors and business partners.

In this instance a Privacy Impact Assessment (PIA) conducted on all data sets within and by each department/agency could provide a baseline inventory of Personally Identifiable Information and identify its location and current security protections.

Once an inventory is available evaluation can be conducted to ensure that each data set is properly classified following information classification standards and appropriate security controls are in place to properly protect the confidentiality of the information and reduce risks to King County.

This undertaking is also large and requires additional dedicated and committed resource, and countywide participation, collaboration and cooperation. It needs to be championed by the County's Leadership at the highest levels.

## Personally Identifiable Information and Privacy in the Constituent Relationship Management System (CRM)

As discussed above in the section entitled Rights and Responsibilities Relating to Protecting Information on page 4 King County collects a large amount of necessary information about residents and others with whom they do business. Certain information that would otherwise be considered personal, and thus confidential, are deemed public information and therefore provided to the government as a matter of course, often times not provided by the "consumer" but by a third party through the filing of documents with the recorder's office.

However King County obtains the information, residents and those engaged in interactions with King County have a right to expect that King County protect this information to the extent allowed by law, and it is King County's responsibility to ensure appropriate protection. Any information recorded about an entity engaged in doing business with King County may be subject to public review, including information recorded in the Constituent Relationship Management (CRM) system. CRM is like any other County system (manual or technological) containing personally identifiable constituent information.

The identifiable information will be protected with appropriate confidentiality and privacy controls and only released after review by the Public Disclosure Officers and/or public records officers responsible for the processing and completion of responses to public disclosure requests within individual county agencies or departments.

**Since the Constituent Relationship Management System (CRM) system will be accessed through a web portal a link to the Privacy Notice will be included in the portal as shown in “Figure 1: King County Privacy Notice Link” on page 7.**

## Conclusion

Protecting “Personally Identifiable Information” in a digital environment is very important, particularly for a public entity. With a twelve-year history of having a Privacy Policy which supports solid privacy principles, and a commitment to protecting such information, King County has an excellent track record of resident information protection.

The Constituent Relationship Management (CRM) system as a public record of an interaction with King County is subject to public review and disclosure. However, using the principles and policies already in place, King County is well positioned to ensure this information is not inadvertently disclosed without proper prior review to allow for application of necessary exclusions. Although the County is in an excellent position relative to protecting Personally Identifiable Information, there are always improvements that can be made, as outlined in the recommendations provided within this report.