To maintain the public’s trust and achieve its mission, the Washington State Department of Agriculture (WSDA) must act as a responsible custodian of the information it collects and holds. As directed by law or regulation, WSDA and its contractors or agents must protect the privacy of individuals and other entities and ensure that confidential or identifying information is protected from inadvertent or intentional misuse and disclosure. WSDA provides appropriate access to confidential data/information in limited situations authorized in law, as needed, to benefit and carry out the agency’s mission.

This policy establishes how confidential information is collected, protected, shared and disclosed. The policy and accompanying procedures:

- Establish a minimum standard for managing the internal agency and external sharing of confidential data/information;
- Allow individual divisions or programs to set more stringent requirements as mandated by specific state or federal law or regulation; and
- Establish that the decision to share confidential data/information is set by individual divisions or programs.
This policy does not apply to personnel files maintained by the Human Resources Office (See POL-HR-202 Personnel Files).

With the exception of personnel files, this policy applies to all confidential data and information held by the agency, regardless of subject matter, source or format. It applies to all WSDA employees, programs, offices and divisions.

1. **WSDA COLLECTS ONLY THAT PERSONAL AND CONFIDENTIAL INFORMATION REQUIRED BY LAW OR NECESSARY FOR PURPOSES OF PROGRAM IMPLEMENTATION, AUTHENTICATION OF IDENTITY, SECURITY OR OTHER NECESSARY AGENCY OPERATIONS**

   • The agency will conduct periodic reviews of retention schedules to ensure that personal and confidential information is retained only for carrying out the purposes for which it was collected, and for the minimum period required by law.

2. **WSDA SECURES RECORDS CONTAINING PERSONAL AND CONFIDENTIAL INFORMATION**

   • Each agency program holding records containing personal/confidential information must review its security procedures at least annually to ensure that records are protected from unauthorized access.
   • Programs must actively discourage customers from sending any personal/confidential information by email to the agency.

3. **THE AGENCY RELEASES CONFIDENTIAL INFORMATION ONLY AS PERMITTED BY STATE OR FEDERAL LAW**

4. **ALL EMPLOYEES MUST READ THIS POLICY AND SIGN AGR-1146, THE WSDA CONFIDENTIALITY AGREEMENT**

   • New employees must sign the confidentiality agreement as part of the new employee packet.
   • Existing employees must sign the confidentiality agreement at least once. If an employee regularly handles confidential or personal information as part of his or her position, the agreement may be updated and signed as a part of the supervisor-employee annual performance review.
   • Signed confidentiality agreements are maintained in the employees’ official personnel files.

5. **STAFF MUST FOLLOW THE AGENCY’S CONFIDENTIAL INFORMATION SHARING PROCEDURES WHEN CONFIDENTIAL INFORMATION IS SHARED OUTSIDE THE AGENCY**

   • When there is a request from outside the agency for access to confidential information, the release of internal data must be approved by the authorized designee responsible for the data and the requestor may be required to complete a confidential data sharing agreement (DSA).
   • Exceptions include:
• When state or federal law provides a different method for release of confidential information.
  • When confidential information is shared within the context of litigation or other administrative proceedings and confidentiality is assured through other mechanisms in law or rule.

- WSDA does not sell, rent, lease or make personal information about individuals available to third parties except in certain circumstances when sharing is required, such as:
  • If the agency is required to share information in order to carry out a legitimate business function of the agency. For example, information about an individual subjected to pesticide exposure may be made available to the state Departments of Health or Labor and Industries.
- WSDA does not give, sell or allow the inspection of lists of individuals to anyone intending to use the information for commercial purposes, unless specifically authorized or directed by law.
  • Requests for any lists for individual names must include all of the following:
    ▪ A completed and signed Form AGR-1006 Request for Public Records. This must include the Agreement to Protect Lists from Use for Commercial Purposes.
    ▪ A written statement attesting that the list requested will not be used for commercial purposes, including a statement of the purpose of the intended use.

6. WHEN ENTERING INTO A CONTRACT OR DATA SHARING AGREEMENT (DSA) WITH PRIVATE OR OTHER GOVERNMENT ENTITIES, SHARED PERSONAL AND CONFIDENTIAL INFORMATION MAY ONLY BE USED FOR THE PURPOSES OF THE CONTRACT

- Any contracts or agreements must clearly state that shared information may not be shared with, transferred, or sold to unauthorized third parties.
- When receiving personal or confidential information from another agency, WSDA will protect it from disclosure in the same manner as the original agency that collected the information, consistent with requirements for disclosure under chapter 42.56 RCW or other state law.
- Contracts and agreements must include provisions to address breach of privacy. Sanctions may include:
  • Return of all personal information.
  • Termination of the contract or agreement.
  • Indemnification to the state.
  • Provisions to hold the state harmless.
  • Monetary or other sanctions.
  • Debarment.
  • Other appropriate ways to maximize protection of citizens’ personal and confidential information.

7. ONLY THE MINIMUM AMOUNT OF CONFIDENTIAL DATA/INFORMATION NECESSARY TO ACCOMPLISH THE STATED PURPOSE SHALL BE RELEASED
8. **STAFF MUST FOLLOW THE AGENCY’S CONFIDENTIAL INFORMATION SHARING PROCEDURES WHEN CONFIDENTIAL INFORMATION IS SHARED WITH OTHER PROGRAMS INSIDE THE AGENCY**

- WSDA programs that share confidential information on a regular basis with other WSDA programs must sign **AGR-1147**, an internal confidential DSA, with the requesting program.
- WSDA programs that request document(s) containing confidential information and do not have an internal confidential DSA with that program must submit the request to the WSDA public records officer for tracking and possible redaction of the confidential information.
- The program that collects and maintains confidential information is responsible for determining whether that confidential information can be released to other programs within the agency.
- Employees must access only the confidential information they have been authorized to use. They must access, use and disclose the minimum amount of confidential information necessary to do their work. They must not otherwise access, use or disclose confidential information except as required under state or federal law.

9. **UNLESS OTHERWISE APPROVED BY THE CHIEF TECHNOLOGY OFFICER, RESTRICTED AND CONFIDENTIAL INFORMATION MUST BE STORED ON DEPARTMENT SERVERS OR SHARED DRIVES THAT ARE DEDICATED FOR THE STORAGE OF CONFIDENTIAL OR RESTRICTED INFORMATION**

- Restricted and confidential information must not be stored on WSDA desktop or laptop computer hard drives, outside the department, or placed on the internet or the intranet or other general electronic release formats until the chief information officer determines that sufficient security is in place and appropriate mechanisms are established to authorize individual user access.
- Confidential information must not be transmitted by email unless encrypted or otherwise protected.

10. **THE AGENCY WEBSITE POSTS A PRIVACY NOTICE**

- The notice contains:
  - A description of the information collected and how it is used.
  - Personal information and the individual’s choice to provide personal information online.
  - Public access to the information.
  - The right to review and correct personally identifiable information.
  - Information on whether cookies and applets are used.
  - Security of the website.
  - Disclaimer.
  - Contact information.

11. **WSDA FORMS REQUESTING INFORMATION INCLUDE A PUBLIC DISCLOSURE STATEMENT**
- As forms are created or revised, and if there is space available on the form, the following statement will be included: “Information collected by WSDA becomes a public record and may be disclosed unless exempted by federal or state law.”

12. PARTICIPANTS IN THE SECRETARY OF STATE’S ADDRESS CONFIDENTIALITY PROGRAM SHALL HAVE THEIR DESIGNATED ADDRESSES BE TREATED AS LEGITIMATE

- WSDA employees may not ask for a program participant’s actual address as a prerequisite for obtaining any product or service from the agency.
- Any questions about the program, as provided for in RCW 40.24.050, may be referred to the public records officer.

13. EMPLOYEES WILL NOTIFY THEIR SUPERVISOR, THE AUTHORIZED DESIGNEE, AND ADMINISTRATIVE REGULATIONS MANAGER OF ANY POTENTIAL OR ACTUAL CONFIDENTIALITY BREACH

- Authorized designees and their designees will cooperate with the administrative regulations manager in investigating the potential or actual breach and take appropriate disciplinary action for violations.
- Violations may result in administrative, civil and/or criminal penalties.
- The deputy director, in consultation with the authorized designee and the administrative regulations manager, is responsible for determining when the department should provide information on violations to the appropriate civil or criminal legal authorities.

DEFINITIONS:

Authorized designee means an assistant director; for assistant directors, or for those who report to the director or deputy director, the authorized designee is the deputy director.

Confidential data/information means any writing containing data/information that an individual or establishment has provided in a relationship of trust, with the expectation that it will not be divulged in an identifiable form. In general, confidential data/information is any data/information that is exempt from public disclosure under either state or federal law. If data/information is exempt from public disclosure, it is confidential and entitled to protection. Data/information exempt from disclosure includes, but is not limited to, information protected under the state Public Records Act (Chapter 42.56 RCW).

De-identification means to edit or remove any identifiers or potentially identifying data/information. De-identification may involve, for example, removing certain items from a data file, blacking out identifying information on a printed document, suppressing data in some cells of a table, or collapsing categories for items in a data file or on a data table.

Personal information means information collected by a state agency about an individual and that is readily identifiable to that specific individual. It includes such things as a person’s name, Social Security number, address, home telephone or personal cell number, personal electronic mail addresses, credit card numbers, debit card numbers, electronic check numbers, card expiration dates,
or bank or other financial account numbers. A domain name or Internet Protocol (IP) address is not considered personal information.

**Writing** means handwriting, typewriting, printing, photostating, photographing, and every other means of recording any form of communication or representation including, but not limited to, letters, words, pictures, sounds, or symbols, or combination thereof, and all papers, maps, magnetic or paper tapes, photographic films and prints, motion picture, film and video recordings, magnetic or punched cards, discs, drums, diskettes, sound recordings, and other documents including existing data compilations from which information may be obtained or translated. [RCW 42.56.010 (4)]