Hartford Foundation for Public Giving

Protection of Confidential Personal Information Policy

Date of Adoption by the Board of Directors: October 5, 2016

Safeguarding Confidential Personal Information related to our employees, job applicants, volunteers, donors or potential donors, or any persons who provide us with that information in the course of their interaction with the Foundation is a fundamental responsibility of each employee, including consultants and agents, and of the Foundation's directors and volunteers.

"Confidential Personal Information" means information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, social security numbers, drivers' license numbers, financial account numbers, credit or debit card numbers, tax payer identification number, passport or alien registration numbers, health insurance information, protected health information, and unique biometric data such as a fingerprint, a voice print, a retina or an iris image, or other unique physical representations. Confidential Personal Information does not include information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

No third-party rights are intended to be created by this Policy. The Foundation reserves the right to amend or change this Policy at any time.

1. *Collection, Storage and Access to Confidential Personal Information*

The Foundation collects Confidential Personal Information only when such information is necessary for the operation of the Foundation's activities.

Confidential Personal Information in electronic form should only be stored on storage media and devices that have been issued or expressly approved by the Foundation for that purpose. Confidential Personal Information maintained in electronic form or transmitted over the Foundation's business system applications will be safeguarded under Foundation proprietary electronic transmission and intranet policies and security systems. The Foundation has implemented internal safeguards to protect any data, computer files, and electronic documents containing Confidential Personal Information. Confidential Personal Information maintained in paper form shall be stored so as to minimize potential misuse and inappropriate disclosure of such information.

Employees are permitted access and use of Confidential Personal Information only as necessary and appropriate to carry out their assigned tasks in the performance of their respective job functions. Access to Confidential Personal Information and other records is based on each employee's job responsibilities. Any employees granted access to

Confidential Personal Information must take all necessary precautions to ensure the integrity of records that include such Confidential Personal Information.

2. *Disclosure of Confidential Personal Information*

It is the responsibility of all Foundation employees, including consultants and agents, directors, and volunteers, who access, use, disclose, collect, verify, review, or maintain files containing Confidential Personal Information, whether the information is in print or electronic form, to do so with strict attention to maintaining the confidentiality of that information. The Foundation strictly prohibits the disclosure of a person's Confidential Personal Information to a third party without the express written permission of the person, unless permitted or required by law, or unless the information has otherwise been made public, in accordance with applicable state and federal law. Prior to disclosure of Confidential Personal Information as permitted or required by law, the Foundation's President must approve such disclosure. For employees, any disclosure of Confidential Personal Information in violation of this policy may result in management action, up to and including termination of employment, and depending on the circumstances, may subject the employee to additional penalties under state or federal law.

Whenever Confidential Personal Information is provided by the Foundation to vendors or subcontractors, including consultants, confidentiality agreements must be executed prior to the release of any such information. A copy of the standard agreement is available from the Vice President for Finance and Administration. Under appropriate circumstances, the Foundation may agree to use a vendor's standard confidentiality agreement as part of a universal contract, provided that the vendor's contract provides comparable protection, with the express written approval of the Vice President for Finance and Administration.

Participants in the Foundation's benefit plans should be aware that Confidential Personal Information will be shared from time to time with plan providers as required for their claims handling or record keeping needs, in accordance with applicable state and federal law.

3. *Reporting and Destruction*

Any director, employee, consultant, volunteer, or other agent of the Foundation who becomes aware of the unauthorized use, access or disclosure of Confidential Personal Information is obligated to report the violation in accordance with the Foundation's Whistleblower Policy. In the event that any mobile or remote computing device (whether owned by the Foundation or otherwise) that stores Confidential Personal Information or that is used to connect to the Foundation's information technology systems is lost or stolen, or is suspected to have been lost or stolen, such incident should be reported immediately to the Foundation's Vice President for Finance and Administration. In

response to any such reports, the Foundation will take action to determine whether the Foundation is required to report a breach of security in accordance with applicable law and Foundation policy.

Foundation records containing Confidential Personal Information shall be kept in accordance with the Foundation's Document Retention Schedule, a copy of which can be obtained from Vice President for Finance and Administration. Except as otherwise required by law, Confidential Personal Information contained on paper, upon disposal, shall be cross-cut shredded, incinerated, or pulped. Confidential Personal Information contained in electronic media (including without limitation, CPUs, copy machines, printers, fax machines and scanning machines with hard drives, tapes, USB-type drives, disks and external hard drives) shall be rendered unreadable upon disposal or upon the return of leased media.

Any employee failing to comply with applicable safeguards may be subject to management action, up to and including termination of employment.

4. *Application to Personnel Records*

The Foundation complies with applicable state and federal law pertaining to the protection of personnel records. All employment and pre-employment personnel information is maintained in locked, segregated areas and is not viewed by anyone except authorized Human Resources and Administration staff with a legitimate business need. Nothing in this policy is intended to modify an employee's right to access his or her own personnel records in accordance with applicable law.

Adopted by the Board of Directors on October 5, 2016