The Dayton Foundation
Component Fund Website and Privacy Policy
(Governing Board Approval – 09/16/2020)

Purpose:

The Dayton Foundation (The Foundation) must assure that all component funds maintain a secure website, utilize a protected method for collecting on-line credit card gifts and protect Personally Identifiable Information (PII).

Website Policy:

If a component fund of The Foundation chooses to have a website or social media presence it must clearly state that it is a component fund of The Foundation and should visibly display The Foundation's logo with a component fund notation below (see example at the end of this policy. The uniform Resource Locator ("URL") associated with the website must be secure and have an active Secure Sockets Layer ("SSL") certificate. A secure website will have a small lock symbol next to the site's URL. New websites must be approved by The Foundation and must follow all security requirements.

For those component funds utilizing the Foundation's tax identification number and corresponding non-profit status, on line credit card donations may only be accomplished by establishing a link that redirects the donor to the Foundation's credit card donation page. Upon request, this link can be customized to populate the Foundation's donation page with the fund name and number. Utilizing a link to The Foundation's donation page prevents fraud and maintains confidentiality. It also allows for proper record keeping and tax acknowledgment.

All credit card donations made to the Foundation are processed through the Authorize.Net Payment Gateway. This Gateway manages the complex routing of sensitive customer information through secure credit card processing networks. At no time is any personal or credit card information made available to any party. In addition, all check donations to a component fund must be payable to "The Dayton Foundation" with a memo notation listing the component fund name and number.

Only component funds that have their own tax identification number and corresponding non-profit status, may directly accept credit card donations. Only credit card processors that meet Payment Card Industry Data Security Standards ("PCI DSS") may be utilized.

The Foundation provides cyber insurance coverage for all component funds. It is advised that those component funds that process credit cards also carry independent cyber security insurance.

Privacy Policy:

Since 1921, the Foundation has been committed to maintaining the confidentiality, integrity and security of PII entrusted to us by current donors, potential donors, and the officers and staff of not-for-profit agencies who approach us for funding. All component funds must adhere to this commitment. Any PII collected from individuals (e.g., name, address, phone number, e-mail address, date of birth, etc.) is to be used solely by the component fund to facilitate charitable gifts and/or maintain correct contact information. All component funds of the Foundation are prohibited from selling, sharing or trading PII.

All component fund web traffic statistics, including which pages are visited in what order and how long users spend on our site must be used for internal purposes only. This data may be analyzed internally to

determine how to best provide information to web site visitors but at no time may names or personal information collected during the tracking process be sold, shared or traded.

Any component fund with a website that collects PII via registration forms or other means must have proper protections in place. This includes website cybersecurity, sound practices for using and storing PII, and a public privacy policy posted on their website that explains how PII data is utilized. A sample policy is available upon request.