

e-Pledge: Simple, Secure Workplace Giving



e-Pledge is United Way's secure online giving platform, designed to make managing your workplace campaign simple and efficient—from launching your campaign and collecting pledges to tracking results and final payroll reporting.

✉ **Emails will be sent from:** epledge@unitedwayhp.org

Please add this email address to your approved sender list.

Questions? Contact your United Way Campaign Team at **336-883-4127** or visit www.unitedwayhp.org.

Getting the Most from e-Pledge

Save Time

- Eliminate paper pledge forms.
- Reduce manual reporting and data entry.
- Easily track outstanding pledges and follow up with employees.

Stay Secure

- Protect employee information with Extended Validation SSL encryption.
- Allow employees to securely submit payroll deductions or credit card gifts through a personalized link.

Personalize Your Campaign

- Feature your company logo, campaign thermometer, and customized messages.
- Allow employees to view their previous gift, suggested giving level, and update their own information.
- Automatically send a thank-you email after each pledge is submitted.

Monitor Your Campaign

- Access live campaign results anytime.
- Export reports to PDF or Excel.
- View total dollars raised, participation, average gift, and outstanding pledges.
- Receive a final payroll file when your campaign concludes.

Getting Started With e-Pledge

To set up your e-Pledge campaign, please provide the following:

Campaign Materials

- Your current Company/Organization Logo
- Website greeting and reminder messages (United Way staff will share templates with you).

Employee Data File

- Submit a populated Excel or CSV file format including the following information:
- **Required fields are needed to create employee accounts and ensure accurate pledge processing and tax receipts.**

Employee ID number *	First Name *
Work Email Address *	Middle Initial *
Number of pay periods *	Last Name *
Department Name and Number *	Suffix *
	Home Address (including city, state, and zip) *

 **Please share the next page with your IT Department**

SECURITY OVERVIEW INFORMATION - FOR YOUR IT DEPARTMENT

Please review the information below regarding the United Way of Greater High Point e-Pledge Email Communication Service. The Email Communications Service affects campaign-related emails, newsletters, and other forms of email communications used to keep you informed about our work and upcoming events.

The site can be accessed on Microsoft Edge, FireFox, Chrome, and Safari.

📧 **Emails will be sent from: epledge@unitedwayhp.org**

Please add this email address to your approved sender list.

The Email Communication Service sending/originating IP Addresses listed below should be removed from spam filter lists and set as exempt to rate controls. *Not allowing the sending/originating of IP Addresses or not exempting them from rate controls can lead to rejected emails or slow delivery.*

Email Communication Service sending/originating IP Addresses:

52.86.171.35 (smtp1.upicsolutions.net)

34.232.26.125 (smtp2.upicsolutions.net)

34.230.104.208 (smtp3.upicsolutions.net)

156.70.25.157 (associated with mta-70-25-157.sparkpostmail.com)

156.70.25.156 (associated with mta-70-25-156.sparkpostmail.com)

If the Email Communication Service IP Addresses cannot be allowed and exempted from rate controls, several features have been implemented to help reduce the misclassification of email communications from United Way. These features are industry best practices to ensure email deliverability and reduce spam emails. To find out more about these features, please use the URL links provided below.

SPFRecord(SenderPolicyFramework)

This record defines what IP addresses can send emails on the behalf of a domain

<http://www.openspf.org/Introduction>

DKIMSigning(DomainKeysIdentifiedMail)

When an email is sent through the e-Pledge email service, it is automatically signed with a special signature. The receiving party verifies this signature by looking it up a special DNS record. <http://www.dkim.org/#introduction>

DMARC(Domain-basedMessageAuthentication,Reporting&Conformance) DMARC builds on top of SPF and DKIM and helps define what should happen when a message fails checks through SPF and DKIM as well as where to send failure reports. <https://dmarc.org/>

