

DEMOCRATIC PARTY OF EVANSTON

Data Access Code of Conduct and Volunteer Agreement

Effective May 9, 2019

The Democratic Party of Evanston is a nonprofit, member-driven organization managed by its board of directors. Our work is governed under bylaws, as well as by terms of use in our licensing or use agreements for various software platforms which help us marshal information and engage with social media as an organization. The Board appreciates your volunteer service to the organization and to the community we all serve.

As a volunteer for the DPOE, your actions will have a real and important impact on the success of Democrats and the growth of the Democratic Party. As volunteer representatives of the DNC, all volunteers and staff are expected to conduct themselves in a professional and ethical manner, maintaining high standards of integrity and the use of good judgment. Accessing data on individual volunteers, members, donors and voters is intrinsic to our work. This data is confidential information and may contain private, personally identifiable information. DPOE is committed to protecting the privacy as well as the integrity of both the data and the software platforms it uses and that the Democratic Party as a whole provides.

We ask you to abide by the following guidelines. **By accepting this, you certify that you have read and agree with this Code of Conduct and Volunteer Agreement.**

As a volunteer, you will:

- Be polite & respectful even when the voter, fellow volunteers or third-party vendors with whom DPOE does business are not, because you are representing the organization to the public.
- Always assume good faith and be constructive in interactions with staff and volunteers.
- Ask questions if you need help.

VOLUNTEER AGREEMENT

While working with data, software and systems on behalf of DPOE you have the following responsibilities:

- Interact with one another and with members of the public or third-party vendors in a professional, courteous, respectful and equitable manner.
- Perform your volunteer job functions in the best interests of the DPOE.
- Read and conform to the terms of use for any software platforms required for your function whose access is provided via DPOE. Participate in any training offered or required by DPOE related to those platforms, either in person or online.

- Maintain and respect the confidentiality of all information about volunteers, voters, donors and members of the DPOE that you obtain in the course of your participation in DPOE activities and act in compliance with the DPOE Privacy Policy (available online and at the DPOE office). Do not disclose confidential information to anyone without permission of a DPOE Board member or standing committee chair. Even when you are no longer a volunteer with the DPOE, any confidential information you have accessed must continue to be kept confidential.
- When work is performed away from the DPOE office, store all paper copies containing protected data (names with email addresses or with mailing addresses or phone numbers, names with contribution amounts, credit card information) in a closed folder or envelope until it can be returned to the DPOE office or to the committee chair who provided the papers to you and assigned the task.
- When working on your own personal computing device on a DPOE task requiring access to a software platform covered under this Code of Conduct or requiring inputting or working with protected data from paper copies:
 - The device must be password protected using a strong password (at least eight characters and a combination of upper- and lower-case letters, numbers and symbols), and the password must be changed at least every 90 days.
 - The display screen must be shut off when you are not directly working on the task.
 - Other members of your household must not have access to the files you are working on.
 - No access to either software platforms or data files, such as spreadsheets stored in the cloud that you create, may be made through a public WIFI internet connection (as in a café, library, airport or other similar location).

Paper copies containing protected data must be shredded as soon as possible after the data has been transferred to an electronic and more privacy-controlled format. After such data transfer and until the paper copies can be shredded, they will be kept in the DPOE office in a file drawer or closed box appropriately labelled as material for shredding. These papers may be removed from the office for collective shredding at another location such as at a publicly offered, secured document shredding event.

If you suspect or learn that unauthorized access or disclosure of data or your credentials necessary to access data may have occurred, you must notify a Board member of the DPOE or the committee chair who assigned the task immediately, but in no case more than 24 hours after learning of an unauthorized access, disclosure of data or data breach. Notify a Board member of the DPOE or the committee chair who assigned the task regarding any concern you have about data privacy or integrity which may arise in your volunteer work.

Your authorization to serve as a volunteer may be terminated at the discretion of a staff member or Board member of the DPOE at any time if it is determined to be in the best interests of the DPOE. Any breach of these requirements will result in your termination as a

volunteer, immediate revocation of access to volunteer platforms, and may result in legal action against you.

CERTIFICATION

I have read the above Data Access Code of Conduct and any Appendixes attached. I understand my responsibilities, and, by signing below, I agree to abide by the Code of Conduct and Appendixes.

NAME

SIGNATURE

DATE