**MIDTOWN EDUCATIONAL FOUNDATION**

**PRIVACY POLICY**

Midtown Educational Foundation (“MEF”) has adopted this Privacy Policy to set forth the principles to be followed in safeguarding the information related to MEF’s program participants, their families, donors, volunteers and employees.

1. We believe that maintaining the privacy of information related to MEF’s program participants, their families, donors (whether they make their donations online or otherwise), volunteers and employees is important to MEF and its mission. We are committed to maintaining the confidentiality and security of such information, both online and offline. Therefore, we shall maintain physical, electronic and procedural safeguards reasonably designed to protect such information from unlawful or unauthorized disclosure, destruction, loss, change or access.
2. “Protected Information” shall mean information which correlates to and identifies a particular individual and shall include contact information such as street address, e-mail address and phone numbers, income history, donors’ detailed giving histories, academic records, credit card information, and the results of background checks.
3. MEF annually publishes an Annual Report showing giving by tier for the fiscal year. Donors may opt to remain anonymous.
4. Certain MEF employees have a need to know about Protected Information and therefore will have access to such information.
5. We shall not disclose Protected Information to external organizations or persons unless authorized by the person associated with the Protected Information, as required by law or as reasonably necessary for MEF to provide its services to Participants and otherwise to advance its mission.
6. MEF will not trade, share or sell Protected Information (whether obtained online or offline) to any outside party, nor will it mail or e-mail material on behalf of other organizations to its donors.
7. We will use Protected Information in the following manner: to administer the programs of MEF, to determine from time to time whether the programs of MEF are serving their intended beneficiaries, to engage in fundraising and for other reasons in the advancement of MEF’s mission.
8. Nothing in this Policy shall prevent MEF from aggregating Protected Information and using it in a manner that preserves the anonymity of such information with respect to any individual.
9. We shall not sell Protected Information to anyone.
10. We shall treat Protected Information about former program participants, their families, donors, volunteers and employees in the same manner that we treat information about current ones.
11. All employees and volunteers of MEF are responsible for protecting Protected Information.

Each person shall be mindful of this responsibility in the conduct of his or her daily activities. If you observe anything unusual relating to Protected Information, you must report this to your supervisor immediately.

1. Loss of laptops or mobile devices containing Protected Information shall be reported immediately to the Executive Director.
2. Access to premises shall be restricted physically, e.g. by locked doors. MEF’s 718 South Loomis and 310 South Peoria locations are additionally protected by virtue of alarm systems. Only persons with a key or accompanied by a person with a key when entering the premises for lawful reasons may enter the offices outside of normal hours.
3. During normal hours, employees shall at all times have responsibility for monitoring persons entering our locations.
4. Protected Information that is maintained electronically shall be maintained in a password-protected fashion. Any access point to Protected Information that is not password-protected shall be monitored or physically protected.
5. Computers connected to the Internet must have reasonably up-to-date security software.
6. When an employee relationship with us is terminated, such person’s access to our premises and Protected Information shall be terminated as soon as is practical.
7. Agreements with vendors which are expected to have access to Protected Information shall be reviewed to consider the confidentiality provisions included in such contracts.
8. With respect to Protected Information correlating to a resident of the EU, MEF shall, upon request and to the extent feasible, strive to discharge the rights in favor of data subjects under the GDPR, including, among others, the right to receive detailed information on use of such information, the right of access to such information, the right to amend any inaccuracies in such information, and the right to erase such information.
9. All employees shall review this policy and indicate their understanding of it by signing an acknowledgment.
10. MEF shall from time to time conduct training on this Policy. Orientation sessions for new employee orientation shall include information about this Policy.
11. If an information security breach is detected, the Executive Director shall be notified immediately. If a material information security breach has occurred, the Executive Director shall immediately notify the President of the Board of Directors. The Executive Director shall also determine which other parties should be notified of the breach, which may include the board, auditors, legal counsel, governmental bodies and the person(s) associated with the Protected Information. The Executive Director shall promptly consult with IT consultants to determine the cause of the breach and to take steps to remediate the breach as soon as possible. S/he shall also determine what steps should be taken to minimize the risk of such a breach happening in the future.
12. The Executive Director shall monitor compliance with this Policy and at least annually shall review the policy with a view towards keeping it updated to reflect changing practices and legal requirements.

Effective: September 17, 2018

Revised March 18, 2022