Data Security Tips

Tips for Protecting Your Data Within your Department

- Restrict access to data files (including donor and prospect information) to only those employees who require access.
- Ensure any printed/paper files are kept in a locked file cabinet or secure room.
- Educate development staff and fundraising volunteers, including trustees and board members, on the process and purpose of prospect research and their roles in protecting the data.
- Develop an implementation plan for data use and clearly outline who has access and what data should be entered into your donor management system (DMS).
- Don’t share passwords for your online research tools or your FTP site(s) unless necessary. Only share this information with employees who need to know the information. In cases of staff turnover, be sure to change passwords that grant access to sensitive data.
- Use encryption technology on computers that house or use confidential data on a regular basis.
- Outline consequences for data theft or negligence.
- Protect from outside technology threats such as computer viruses or phishing scams by updating anti-virus and anti-spam software regularly.
- Keep all data, including copies of checks and financial transactions, only as long as required.
- Properly dispose of electronic and hard copies. Be sure to use a shredder when disposing of hard-copy data so that the information remains confidential.

Tips for Protecting Your Data When Sending Data to a Vendor

- Ensure that a single person on your staff is responsible for file submission.
- Only include data that is relevant to the service that the vendor provides.
- Do not transfer data via email; use secure methods such as file encryption or SFTP.

Tips for Protecting Your Data When Communicating with Constituents

- Be up front about your prospect research. Consider posting a statement on your website or in your public privacy policy about data mining. Transparency up front helps assuage issues later.
- Develop a policy statement outlining process/policies/FERPA compliance to be distributed to constituents who question research processes or practices.
- Allow constituents an opt-out option for fundraising activities.