Our Commitment to Privacy and Security

Nonprofit organizations in every industry rely on iWave to support their fundraising operations, and we take that responsibility seriously. That's why we are focused on providing industry-leading security and privacy capabilities, along with transparency of our data partners and visibility into how client data is managed. It's our commitment to you. Here's how we're working every day to earn and maintain your trust.

When you use iWave, you can be confident that:

We never share your data.

As an iWave client, you own your data. Client data is the data you, both your organization and your users, provide to iWave including profile details, internal giving data, screening projects and analytics. Client data is not shared in any way with third-party organizations or other clients.

We follow industry-standard security frameworks and certifications.

iWave is regularly audited by third-party experts and holds a SOC 2 certification.

We are compliant with industry privacy standards and regulations.

These include the California Consumer Privacy Act (CCPA), the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA) and the Federal Election Campaign (FEC) Act. This is why iWave, unlike other platforms, does not use FEC political giving in scoring algorithms and profile record matching. FEC regulations expressly prohibits use of contribution data for soliciting contributions, including charitable contributions. More information about FEC guidelines can be found by clicking here. We also provide the ability for individuals to request an opt-out of our VeriGift donations database.

We are transparent about our data providers and partners.

All of our data providers and technology partners have completed a rigorous vetting process to ensure compliance with privacy regulations. Known third-party data vendors selling social media information are not compliant with CCPA, which is why iWave does not provide this type of data.

Your privacy is an ongoing priority for iWave.

We complete regular and ongoing data privacy and regulation assessments of our platform, policies and procedures to ensure we are staying up to date with best-in-class practices.

We do not use your data for benchmarking or machine learning.

None of our algorithms or machine learning processes are based on previous results from screening or searches and we do not use your data for benchmarking purposes.

Security is a primary design criteria for our platform.

We build the most powerful security technologies into our platform. In addition to secure coding practices, cybersecurity tools and encryption mechanisms, iWave offers multi-factor authentication (MFA) to protect your username and password. This feature prevents unauthorized access by requiring at least two forms of verification to prove your identity.

We proactively protect your data.

iWave implements stringent security measures to safeguard your data. These include continuous vulnerability scans, penetration testing, ongoing risk assessments and adapting quickly to changes in industry standards, regulations and best practices through partnerships with leading global security experts. We have also chosen the world's most comprehensive and broadly adopted cloud computing environment, Amazon Web Services (AWS), which has a data center and network architecture built to meet the requirements of the most security-sensitive organizations.

Still have questions? Contact info@iWave.com or call 1 800-655-7729.