



PRIVACY AND DATA USE NOTICE

This Privacy and Data Use Notice (“Notice”) explains how information is handled when you access a program portal that uses Neighborly Software. Neighborly Software is a secure, cloud-based platform operated by Benevate, LLC (“Benevate,” “we,” “us,” or “our”) and used by government agencies and other organizations to administer programs. By using the portal, you acknowledge that your information will be handled as described in this Notice.

1. Applicability. This Notice applies to all individuals who access the Software, including:
 - Portal Users: Individuals who access a Client’s portal to apply for or participate in a program, and who are not designated as Subscription Users.
 - Subscription Users: Individuals designated and authorized by a Client to access the administrative or operational portions of the Client’s portal for purposes of program administration.
2. Our Role. Neighborly Software is a technology platform made available to a governmental entity, nonprofit organization, or other authorized organization (“Client”) to administer one or more programs. The Client determines:
 - What information is collected
 - The purposes for which information is used
 - Eligibility, funding, and policy decisions
 - Retention requirements under applicable law

Benevate provides and supports the Software but does not administer Client programs and does not make programmatic or eligibility decisions. We handle information submitted through Client portals only to operate, maintain, and secure the Software on behalf of the Client.
3. Information Submitted Through a Portal. Information submitted through a Client portal may include the following:
 - Name
 - Address
 - Email address
 - Telephone number
 - Date of birth
 - Employment information
 - Financial or eligibility-related information
 - Social Security number or bank account information (if required by the Client’s program)
 - Other information required by the program



Benevate applies administrative, technical, and physical safeguards to protect all information processed through the Software.

4. Information Automatically Collected. When you access a Client portal, certain technical information is collected automatically to help keep the system secure and functioning properly. This may include:
- IP address
 - Browser type and version
 - Device and operating system information
 - System activity logs

This information is used to protect against unauthorized access, detect fraud, maintain system performance, and provide technical support.

5. Data Ownership and Use. All information submitted through a Client portal is owned by the Client administering the program. Benevate does not claim ownership of that information. We do not sell, rent, or trade your information, and we do not use identifiable information for advertising or marketing purposes. We use information to operate, secure, support, and improve the Software on behalf of the Client. We may use information that has been aggregated or de-identified so that it cannot reasonably identify an individual or the Client for business purposes, including analyzing platform performance, improving our services, and describing the utilization of the Software generally.
6. How Information Is Shared. Information may be shared in limited circumstances:
- To the Client. The Client administering the program has access to submitted information and determines how it is used and retained.
 - Service Providers. Benevate may use trusted third-party providers (such as hosting providers) to operate the Software. These providers are required to protect information and may use it only as necessary to support the platform.
 - Legal Requirements. Benevate may disclose information when required by law, subpoena, court order, or lawful governmental request. Where permitted, Benevate's standard practice is to notify the Client.
7. Security Measures. Benevate maintains a comprehensive information security program designed to protect information from unauthorized access, use, alteration, or disclosure. We regularly review and update our security practices to address evolving risks. Our safeguards include measures such as:
- Unique login credentials
 - Role-based access controls
 - Encryption of data in transit and at rest
 - Secure hosting environments
 - Monitoring and incident response procedure



8. Account Security. Users are responsible for maintaining the confidentiality of their login credentials and for activity that occurs under their accounts. Please use strong passwords, avoid sharing your credentials, and log out when using shared or public devices. If you suspect unauthorized access to your account, notify program staff or contact Neighborly Software Support by selecting the Help icon within the portal or emailing us directly at Support@NeighborlySoftware.com. Benevate will never ask you to provide your password by email, phone, or other unsolicited communication.
9. Access to Your Information. If you have questions about your information, need assistance accessing it, or wish to request corrections or other actions, please contact program staff. Benevate supports the Client in responding to such requests in accordance with applicable law and the Client's instructions.
10. Data Retention. Information is retained in accordance with the Client's instructions, applicable laws, and the terms governing Benevate's provision of the Software to the Client. Government Clients may be subject to public records or record retention laws that determine how long information must be maintained.
11. Updates to This Notice. We may update this Notice from time to time. Updated versions will be posted within Client portals, and the "Last Updated" date will reflect the revision date. Any updates will apply on a prospective basis and will not materially reduce the privacy or data protection obligations applicable to Client Data as set forth in this notice or in our applicable contractual commitments to Clients.