

Maryland's Department of Service and Civic Innovation Privacy Notice

Last Updated: (September 25, 2026)

Table of Contents:

- [1. Introduction](#)
- [2. What Personal Information We Collect](#)
- [3. Why We Collect and Process Your Personal Information](#)
- [4. Knowledge and Consent](#)
- [5. Limiting Collection](#)
- [6. Use, Disclosure, and Retention of Personal Information](#)
- [7. Accuracy](#)
- [8. Safeguarding Personal Information](#)
- [9. Privacy Notice Changes](#)
- [10. Access to Personal Information](#)
- [11. Artificial intelligence](#)
- [12. How to Contact Us](#)
- [13. Email](#)
- [14. Website Privacy](#)

1. Introduction

Protecting Your Information

The State of Maryland's Department of Service and Civic Innovation (DSCI) works to protect your personal information. This includes keeping it private, accurate, and secure. We do this by using fair information privacy rules.

What This Document Covers

This document explains:

- How we collect your personal information
- How we use it
- How we protect it
- How we share it

We are responsible for protecting any personal information we control. This notice applies to all personal information we collect, use, and share through our websites, in-person services, and written correspondence.

2. What Personal Information We Collect

We collect and use certain personal data about you to administer state service pathways, partner relationships, member eligibility verification, and grant/stipend processing. Here's what we gather:

- **Member & Applicant Data:** Full name (including given and surnames), home address, telephone number, email address, Social Security Number (SSN), citizenship status, date of birth/age verification, government-issued photo ID, demographic information, emergency contact details, educational history, and program participation/attendance milestones.
- **AmeriCorps Member Compliance & Benefit Records:** National Service Criminal History Check (NSCHC) documentation (including NSOPW searches, Truescreen/state repository checks, FBI fingerprint/Fieldprint orders, case adjudication notes), Member Service Agreements, reasonable accommodation requests, health insurance enrollment/waiver forms, child care benefit forms, member timesheets (tracking service, training, and fundraising hours), mid-term/end-of-term performance evaluations, disciplinary memos, and eGrants exit/Segal Education Award certification forms.

- Host Site Partner Data: Primary contact names, business addresses, professional phone numbers, business email addresses, Federal Employer Identification Numbers (FEIN), and host site supervisor details.
- Financial & Grant Processing Data: Direct deposit bank routing/account details for stipend distribution, grant award amounts, disbursement history, and financial verification records.

We follow official State and federal laws to collect your personal information and protect your privacy while providing these services. These laws include:

- [Health Insurance Portability and Accountability Act \(HIPAA\)](#)
- [Criminal Justice Information Services \(CJIS\) Standards](#)
- [Financial Tax Information \(FTI\) rules governed by the IRS](#)
- [Maryland Data Privacy and Protection Act of 2026 \(HB 264\)](#)
- [Maryland Public Information Act](#)

3. Why We Collect and Process Your Personal Information

a. Why We Collect Your Information

We collect, use, and share your personal information to decide if you qualify for specific state services, benefits, or products, such as participating in the Maryland Corps/Service Year Option program as a member or host site partner and to receive associated grant awards and stipends. We also collect financial or sensitive data to complete specific transactions you request.

We may offer you chances to apply for other helpful State programs. Sometimes, the reason we need your data is obvious. For example, if you give us your name and payment information for an application, we assume you agree to let us use it for that service.

b. How We Use Your Information

We collect and use your personal information to check if you qualify for the benefits or services you've asked for. This might include financial or sensitive information if needed to process your application.

What We Do with Your Information

- Legal and Regulatory Compliance: We use your information to meet laws and regulations, support audits and investigations, prevent fraud, and improve our programs and operations.
- Other Opportunities: We might inform you about programs from other agencies that could help you.

- **Service Improvements:** We also use data to analyze and enhance State services and to stay compliant with the law.
- **Sharing Information:** Where allowed by law, we might share information with other government agencies or authorized entities for these purposes.

We only use your personal information as needed for these purposes and follow privacy and data protection laws.

4. Knowledge and Consent

We will let you know and get your okay before we gather, use, or share your information, unless the law lets or requires us do it without asking. We will tell you why we need your information before or when we ask for it. When you provide information like your address or payment details as part of an application, we consider it your permission to use that data for that specific purpose.

Choosing to give us your information is up to you. But without it, we may not be able to provide the services you want. We won't make you agree unless the law requires it or it's necessary for the service. When you sign a form or select "I agree" online, it means you officially allow us to use your information.

5. Limiting Collection

We have rules to limit the data we collect. We only gather the personal information needed to do our job.

If we get your information from another source, like the government or a verification company, we use legal agreements. This ensures we only get what the law or contract requires.

6. Use, Disclosure, and Retention of Personal Information

Use of Your Data: We use your data only for the purpose it was first collected, unless you give permission, for legitimate government purposes, or the law demands it. We keep your information only as long as needed to complete that task, following State record timelines.

Sharing Your Data: We might share your data with contractors (such as our application portal and CRM software providers) who help us with your requests. Additionally, limited personal information (such as applicant names, contact information, and placement details) is shared with authorized host site partners to facilitate program placements and operations. These contractors and partners must sign strict contracts and agreements to keep your data secure and confidential. We never sell your personal information to anyone.

Anonymizing Your Data: To better serve you, we might remove your name and details to make your data anonymous. Under formal Data Use Agreements (DUAs), we share this anonymized data with designated research and evaluation partners, as well as other Maryland State agencies, for research, program evaluation, and service performance measurement. We use advanced tools and privacy-enhancing practices to block your identity, so agencies and researchers can study trends and program outcomes without seeing your private details.

Public Access to Records: Government records may be open to the public if required by the Maryland Public Information Act . However, Maryland law has safety exceptions to keep your private details from being released to the public.

7. Accuracy

We make sure your information is correct, complete, and current. We might ask you to verify your details.

Under the Maryland Public Information Act , you can ask us to fix mistakes, update old facts, or add missing information to your records. It's your job to provide us with accurate details and let us know when your information changes.

8. Safeguarding Personal Information

Protecting Your Data: State and federal laws require DSCI to safeguard your information. We protect your data in compliance with the Maryland Personal Information Protection Act, federal privacy standards (including HIPAA for health-related records where applicable), and the Maryland Department of Information Technology (DoIT) Information Security policies. We employ multi-layered security controls, including enterprise-grade encryption (in transit and at rest), strict role-based access controls, secure cloud environments, and monitored physical storage systems.

What Happens if Someone Accesses Your Data Unauthorized: If we discover or suspect that your personal information has been accessed, acquired, or disclosed without authority, DSCI will execute our formal Incident Response Plan. In accordance with Maryland law, we will promptly investigate the incident, notify the Maryland Office of the Attorney General, coordinate with the State Chief Information Security Officer (CISO), and directly notify impacted individuals in writing or electronically with details on the incident and protective measures available.

9. Privacy Notice Changes

We check and update this notice at least once a year to keep up with new laws, technology and best practices. We will let you know about any big changes by posting the new rules with a new "Last Updated" date.

10. Access to Personal Information

Requesting Your Information: You can ask us to share what information we have about you and how it is used. You have the right to request to review. You can ask us to change or delete data you provided directly, depending on State laws. If the data came from another source, you must contact that source to change their files.

What We Can't Show You: Sometimes, we can't show you certain files because of the law. We can't show you records that include:

- Private data about other people
- Files restricted by police or law enforcement
- Information covered by official security rules

If We Deny Your Request: If we have to deny your request, we will explain why in writing and keep a record of it.

11. Artificial intelligence

AI Technology is becoming more common. We may use it directly and indirectly in providing services to you.

Direct Interaction with AI: When seeking services or applying on our workforce platform (Build Within), applicants may interact directly with a Virtual Interviewer Component (VIC) to validate application responses and determine whether applicants meet the basic requirements for program eligibility. Additionally, users may interact with an AI coach (Maestro AI) to receive personalized career guidance, skills gap insights, and multi-language support.

Indirect Interaction with AI: Indirect use includes our platform's use of automated algorithms and AI agents to objectively match applicant competencies with available host site placement opportunities and career paths.

Our Commitment to You: We are committed to being clear and open when you use AI. All AI tools utilized by DSCI operate with strict human-in-the-loop oversight. DSCI staff systematically review all VIC interview results and eligibility assessments before final determinations are made. Additionally, our AI infrastructure incorporates continuous bias testing and robust data encryption. We follow Maryland's Responsible AI Policy to protect your data.

12. How to Contact Us

You can ask questions about this notice, request data, or report a privacy issue by contacting our Privacy Team. You can contact:

Rosy Branson, DSCI Chief Information Officer

Email: rosy.branson@maryland.gov

Address: Maryland Department of Service and Civic Innovation 45 Calvert St., Annapolis, MD 21401

13. Email

If you email us, we will use your message to answer your questions. Your emails are like official letters. They can become public records and may be shared if someone asks for them under the Maryland Public Information Act.

14. Website Privacy

This section explains privacy practices related to our website(s).

a. Cookies

A cookie is a small file saved on your computer when you visit a website. We use cookies to help our site work well, count visitors, and make your experience better. Most web browsers accept cookies by default. You can change your settings to block cookies, but doing so might stop some features from working.

b. Information Collected and Stored Automatically

When you visit our pages or download files, our systems automatically collect some basic information. This information does **not** identify you personally. Here's what we collect:

- Your internet domain (like Maryland.gov) and your device's (e.g., computer, phone) IP address. An IP address is a special number given to your device by your internet service provider. This helps your device talk to others on the internet
- The type of web browser (e.g., Chrome, Safari) and operating system you are using
- The date and time of your visit
- The specific pages you view
- Where you click on the site (not including any text you type in forms)

We use this data to improve our websites, to learn about the number of visitors on our sites, and to understand what technology people are using. We do not track or record personal information about individual visits.

c. Other Websites

We link to websites that are not part of the Maryland government. Our privacy rules do not apply once you leave a Maryland.gov site. We can't control how these other websites use your data. Always check their privacy statements to understand how they handle your information.

d. Site Security

To protect our websites and make sure they are accessible to everyone, we use special security tools. These tools watch the traffic on our network. They help us find and stop any attempts to change data or harm our pages.

We do not try to find out who individual users are unless it is part of a police investigation. Uploading unauthorized information or damaging government computer systems is against the law. This can lead to punishment under both State and federal laws. In the event of a data breach, we will notify the impacted individuals according to the law and our data breach plan.