

Members 1st Federal Credit Union Employee and Applicant Privacy Policy

FACTS	WHAT DOES Members 1st Federal Credit Union DO WITH THE PERSONAL INFORMATION OF EMPLOYEES AND APPLICANTS?
Why?	We collect, process, and may disclose personal information about you to consider you for employment opportunities, manage your employment with us, and provide benefits to you. For the full list of reasons we use or disclose personal information, see below.
What?	We collect information that identifies, relates to, describes, references, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular employee, household, or device (" personal information "). For specific types of personal information we collect, see below.
How?	We collect personal information directly from you when you provide it to us, on our own when we generate it through the course of your employment, and indirectly from you based on actions you take or through other administrative processes.

This Privacy Policy applies to personal information Members 1st Federal Credit Union ("**Members 1st**," "**we**," or "**us**") collects about our employees and job applicants online and through our website <https://www.members1st.org/> (the "Website"), in paper form, over the phone, through electronic messages between you and us, and from third parties, including our subsidiaries and affiliates (if they collect it on our behalf).

Personal Information We Collect About Employees and Applicants

We collect personal information that includes the following:

PERSONAL INFORMATION WE COLLECT	Examples
Identifiers , such as:	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.
Personal information categories listed under applicable law:	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.
Protected classification characteristics under state or federal law:	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or

	military status, genetic information (including familial genetic information).
Biometric information , such as:	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.
Internet or other similar activity , including:	Browsing history, search history, and activity on systems or devices (including messages and communications).
Professional or employment-related information , for example:	Current or past job history or performance evaluations.
Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.
Inferences drawn from other personal information, such as:	Profiles reflecting your preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes
Government identifiers that are considered sensitive, including:	Social security, driver's license, state identification card, or passport number.
Complete user account credentials , for example:	Username, account numbers, or card numbers combined with required access/security code or password.
Additional information , which may include:	Union membership; mail, email, or text message content not directed to us; unique identifying biometric information; and health, sex life, or sexual orientation.

How We Collect Personal Information About Employees and Applicants

We collect personal information in multiple ways, including:

HOW WE COLLECT PERSONAL INFORMATION	Examples
Directly from you:	When you submit employment applications or complete forms as part of the hiring, promotion, or transfer process.
Generated by us:	When we create employment records (for example, performance evaluations and assessments).
Indirectly from you:	When data is generated by your actions and activities, and through administrative processes like background checks.

Why We Collect Personal Information of Employees and Applicants

We may **collect**, **process**, and **disclose** the personal information of employees and applicants **for the following reasons**:

- To fulfill or meet the reason you provided the information. For example, when you apply for employment with Members 1st, we will use your personal information to consider your application and fitness for the position. Additionally, once hired, we will use your personal information to process your payroll and any benefits you may be eligible for.
- To manage your attendance and entry of time worked.
- To provide and administer payroll and retirement plans, as applicable.
- To provide and administer health and life insurance and other benefits.
- To maintain equal opportunities for all individuals.
- To provide, support, personalize, and develop our human resources services.
- To contact others in the event of an emergency.
- To create, maintain, customize, and secure your internal user account with us.
- To make certain information available on internal company resources and to facilitate communication between and among employees within Members 1st.
- To process your requests and transactions, including for expense reimbursement, and to prevent transactional fraud.
- To manage training and appraisal programs, including the maintenance of performance and disciplinary records.
- To provide you with support and to respond to your inquiries, including to investigate and address your concerns and monitor and improve our responses.
- To help maintain the safety, security, and integrity of our website, services, databases and other technology assets.
- For testing, research, analysis, and product development, including to develop and improve our systems, products, and services.
- To conduct employee and staff surveys.
- To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations, including without limitation:
 - To maintain the ethics hotline;
 - To respond to governmental inquiries or requests from public authorities;
 - To comply with valid legal process or discovery obligations;
 - To protect the rights, privacy, safety, or property of Members 1st, its workers, or the public if such a disclosure is proportionate in the individual case;
 - To permit Members 1st to pursue available remedies or limit the damages that we may sustain;
 - To respond to an emergency; and/or
 - To comply with applicable regulations, policies, and procedures.
- As described to you when collecting your personal information or as otherwise set forth in applicable state privacy law.
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by us is among the assets transferred.

Disclosure of Personal Information of Employees and Applicants

We may disclose personal information to third parties, including service providers, subsidiaries, affiliates, and/or government agencies as needed to fulfill our specific business purposes. We

do not sell the personal information of our employees or applicants, and we will not share phone numbers or other contact information with third parties for marketing or promotional purposes.

Children Under the Age of 18

Our Website is not intended for children under the age of 18, and we do not knowingly collect the personal information of employees or applicants under the age of 18. No applicant or employee under the age of 18 may provide any personal information to us on the Website or through any other means. If we learn we have collected or received personal information about an applicant or employee under the age of 18, we will delete that information. If you believe we might have any information from or about an applicant or employee under the age of 18, please contact us at 800-237-7288.

Accessing and Correcting Your Personal Information

As an employee or applicant, you may request access to or obtain a copy of your personal information using the contact information below:

Ben Saylor	717-458-6934 saylorb@members1st.org
Careers Portal	https://careers.members1st.org/jobs