

Policy: Data Privacy for Resident Data

Issuing Department: Property Management

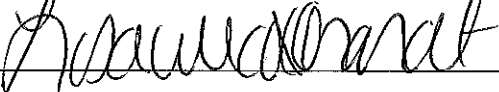
Origination Date: June 2015

Division: Housing and Services
2016

Last Review/Revision Date: September

Created by (Name & Title): Jolene Anderson, Project Manager

Approved by (Name & Title): Lisa Wilcox-Erhardt, Executive Vice President

Approver Signature: 

Approval Date: 9-13-16

1. **Policy Statement:** CommonBond is committed to protecting the rights and privacy of residents we serve, and will use and disclose Resident Personal Information in compliance with applicable laws.
2. **Applicability:** This policy applies to all CommonBond staff and volunteers who acquire, create, use, or disclose Personal Information. Violations of this policy will be handled under CommonBond’s disciplinary procedures.

All staff and volunteers are required to read, understand and follow all policies and procedures that relate to the Personal Information they may handle in the course of their work.

3. Definitions:

- **CommonBond:** means CommonBond Communities, a Minnesota nonprofit corporation, and the following subsidiaries and affiliates: CommonBond Housing, CommonBond Endowment Corporation, CommonBond Investment Corporation, and CommonBond Acquisition LLC.
- **Personal Information:** means (a) individually identifiable information created or received by CommonBond about a Resident, and (b) information with respect to which there is a reasonable basis to believe the information could be used to identify the Resident. Personal Information includes, but is not limited to, demographic information; income and asset data; physical and mental health information; financial data, such as account numbers; social security numbers; and family information. Personal Information includes Private Data.
- **Private Data:** means Personal Information that under the Minnesota Data Practices Act is considered not public, but is accessible to the individual subject of the data.
- **Resident:** means an individual who applies for or receives housing or services from CommonBond.

4. **Contacts:** Questions and comments about this policy may be referred to CommonBond’s Executive Vice President or his or her designee. CommonBond will not retaliate against individuals who in good faith ask questions about or report potential violations of this policy.

- 5. Implementation:** CommonBond staff and volunteers must follow the procedures below and adhere to the other policies and procedures referenced in this policy. CommonBond reserves the right to make changes to this policy and its related policies and procedures and to adopt new policies and procedures as it determines necessary or desirable.

A. Overview

CommonBond will develop and implement a program to protect the privacy and security of Personal Information and protect Resident rights with respect to Personal Information. The program will comply with applicable law and be tailored to the types of Personal Information CommonBond creates and receives. The program will include policies and procedures, training of CommonBond staff and volunteers, and a monitoring and reporting system to detect and mitigate improper uses and disclosures of Personal Information.

The objectives of this Policy are implemented in part through CommonBond's other privacy and security policies and procedures, which are referenced below. CommonBond staff and volunteers must follow all applicable policies and procedures.

All CommonBond staff, and any volunteers who will have access to Personal Information, will receive and review this Policy during New Employee Orientation. Annually all CommonBond staff will review this Policy. CommonBond will retain a signed confirmation of the review in the employee's personnel file.

B. Privacy

General Standard. CommonBond will protect the privacy of Personal Information and will acquire, collect, use, and/or disclose Personal Information only as permitted by applicable federal and state law, including (as applicable) the federal Privacy Act, applicable state health records laws, public records laws, and data breach notification statutes. CommonBond staff who are subject to specific data privacy obligations because of their licensure status, as a social worker, marriage and family therapist, or other health care practitioner, are responsible for complying with all provisions of their licensure statute that regulate the use of client information.

If CommonBond makes representations to a Resident about how the Resident's Personal Information will be used and disclosed, CommonBond will use and disclose the Personal Information only as described in the representations made to the Resident.

Internal Uses. As needed to perform their job duties and as permitted by applicable law, CommonBond staff and volunteers may, without Resident authorization, use and share Personal Information within CommonBond. CommonBond staff and volunteers who have no business need to access or use Personal Information must not access the information. Personal Information will be used only for the purposes for which it was created or collected.

CommonBond staff will use only the minimum necessary Personal Information to accomplish the applicable task. For example, if it is sufficient to use a Resident's name and address, rather than full demographic and financial information, staff will use only the name and address.

CommonBond staff and volunteers will take care to maintain the privacy of Personal Information within CommonBond. For example, oral communications about Residents

generally should not occur in public areas where other Residents, staff or visitors may overhear the conversation. Personal Information in written form should not be left in public places or places where individuals who do not need to see the information might access it. In all circumstances where Personal Information is shared, staff will show respect and take appropriate steps to maintain the dignity of the Resident.

External Disclosures. CommonBond will disclose Personal Information to third parties only in accordance with a Resident's written authorization or as permitted or required by applicable law. If a disclosure is made under an authorization, CommonBond will disclose only the information described in the authorization.

Examples of situations in which Personal Information may be disclosed without a Resident's authorization include, but are not limited to, the following:

- Vulnerable adult and maltreatment of minors reporting
- Disclosures compelled by court order or similar compulsory process
- Other disclosures to government agencies in accordance with applicable law
- Disclosures to prevent harm to the Resident or other individuals
- Disclosures to subcontractors and vendors of CommonBond who need Personal Information to provide services to CommonBond

CommonBond will take appropriate action to inform third parties (including vendors and subcontractors) to whom CommonBond discloses Personal Information of the applicable limitations on the use and re-disclosure of the Personal Information. As appropriate under the circumstances, CommonBond will obtain assurances from the recipient that the recipient will maintain the privacy of the Personal Information, use and disclose the Personal Information only for permitted purposes, and notify CommonBond of any unauthorized use or disclosure of the Personal Information. Where appropriate, CommonBond will ensure that the third party returns or securely destroys the Personal Information once the recipient no longer needs the information.

Third Parties and Data Privacy

CommonBond may have relationships with third parties in order to meet business needs. Third party relationships include any agreement, contract, or pay for service situation with a vendor, organization, company, or individual that does work or provides a service at our sites or with and for residents. This includes third parties working with CommonBond staff to deliver a service.

CommonBond staff must ensure that third parties only access resident Private Data when it is required to fulfill a job. If a third party has access or potential access to resident Private Data a CommonBond Service Provider Contract must be completed. A CommonBond Service Provider Contract must be completed every time when services are provided by an organization other than CommonBond.

De-Identification. If permitted by applicable law, CommonBond may de-identify Personal Information and use and disclose the de-identified data for any purpose.

C. Security

General. CommonBond will provide reasonable security for the Personal Information in accordance with applicable law. CommonBond will take steps to (a) maintain the confidentiality, integrity, and availability of the information; (b) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and (c) protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required. CommonBond will identify a staff member to oversee the organization's data security program. CommonBond staff and volunteers must follow all security policies and procedures implemented by CommonBond.

CommonBond staff and volunteers should minimize travel with Personal Information and transport paper files only when absolutely necessary. If CommonBond staff or volunteers must transport Personal Information, they will take appropriate steps to secure the information prior to and during the transport.

Electronic Personal Information. At appropriate intervals, CommonBond will perform a security risk assessment with respect to electronic Personal Information and take steps to mitigate the identified risks to the security of the information.

CommonBond will implement physical, technical, and administrative safeguards to protect the security, integrity, and availability of electronic Personal Information. These safeguards may include, but are not limited to:

- Physical security and access controls
- Workstation security controls and automatic logoff
- Password controls and log-in monitoring
- Protection against malicious software
- Limitations on the use of unencrypted email and mobile devices
- Contingency plans, such as data backup, retrieval, emergency mode operation and disaster recovery plans

Under no circumstances will CommonBond staff download electronic Personal Information to personal electronic devices or access electronic Personal Information outside the office without the prior permission of their supervisor or another member of CommonBond management.

Security Breaches. If CommonBond learns of an unauthorized use, access, or disclosure of Personal Information, CommonBond will investigate the incident to determine whether it violates applicable law and whether any notification to the individual or any government agency is advisable or legally required. CommonBond will review the following information:

- a. The nature and extent of the information involved, including the types of identifiers and likelihood of re-identification;
- b. The unauthorized person who used the information or to whom the disclosure was made;
- c. Whether the information was actually acquired or viewed; and
- d. The extent to which the risk to the information or the Resident has been mitigated

If notification is advisable or legally required, the Executive Vice President or his or her designee will oversee the preparation and submission of the notice.

CommonBond staff who inappropriately access, use, or disclose Personal Information or who become aware of another person's inappropriate access, use, or disclosure of Personal Information must report the incident to the Executive Vice President within 24 hours. Staff and volunteers must cooperate with any investigation of the incident.

Destruction. CommonBond will ensure that all Personal Information is securely destroyed. For paper records, CommonBond will use methods such as shredding, burning, or pulverizing to ensure the information is rendered unreadable and unable to be reconstructed. Redaction is not considered a secure method of disposal. For electronic information, CommonBond will clear (overwrite media with non-sensitive data), purge (degauss or expose the media to a strong magnetic field), or destroy (disintegrate, pulverize, melt, incinerate, or shred) the media.

D. Resident Rights

General. CommonBond is committed to respecting the rights and dignity of its Residents and will follow applicable laws intended to protect the rights of CommonBond Residents with respect to their Personal Information.

CommonBond will provide information to Residents about the use and disclosure of their Personal Information. Where required by law, CommonBond will inform the Resident under what authority Personal Information is requested, whether the disclosure is mandatory, the principal purpose for which the Personal Information is intended to be used, and the routine uses of the Personal Information. When a Resident moves into a CommonBond property, CommonBond will present a Notice of Private Data Disclosure form to the Resident and ask the Resident to sign and return the form. If the Resident refuses to sign, this will be noted on the Disclosure form and placed in the Resident's file. If applicable law prohibits CommonBond from requiring consent to disclose Personal Information as a condition of program eligibility, CommonBond will abide by that prohibition. The Notice of Private Data Disclosure will be reviewed annually with residents.

Access. In compliance with applicable laws, CommonBond will provide access to a Resident of the Personal Information maintained by CommonBond concerning the Resident. CommonBond may require Residents to make a written request for access in a format acceptable to CommonBond. CommonBond will strive to respond to requests for access within 10 business days, or within the time frame established by applicable law. CommonBond will retain a copy of the written request in the Resident's file. CommonBond may charge a fee for copying records. A staff person must be present during the review and will make an entry in the record as to who accessed the record, date and time of the review, and list any copies made from the record. Staff should consult with their manager each time a Resident requests to view or copy their Personal Information.

CommonBond may deny access to Personal Information if the access request, in the judgment of CommonBond staff, is reasonably likely to endanger the life or physical safety of the Resident or another person.

Amendments. Residents may request amendments to their Personal Information in writing in a format acceptable to CommonBond. If the Personal Information is inaccurate or incomplete, CommonBond will amend the Personal Information to make it accurate and complete.

CommonBond has no obligation to amend information that was not created by CommonBond. CommonBond will strive to provide a response to a Resident's request to amend the Personal Information within 10 business days, or within the time frame established by applicable law.

Restrictions. Residents may request that CommonBond restrict use and disclosure of their Personal Information. Requests must be made in writing in a format acceptable to CommonBond. CommonBond will either grant or deny such a request, and document the request and the response in the Resident's record. If CommonBond grants the request to restrict the use and disclosure of the Personal Information, CommonBond will abide by it, except in the case of a medical emergency or as otherwise permitted or required by applicable law.

6. Related Policies & References: The following policies and procedures support the implementation of this policy. CommonBond may revise these policies and procedures and add new policies and procedures at any time.

- Notice of Data Privacy Practices and Instructions
- CommonBond Communities Service Provider Contract
- CommonBond Communities Social Media Policy
- IT Policies
- Release of Information form
- Informed Consent form
- Minnesota Data Practices Act
- Minnesota Health Records Act
- HUD regulations and guidance for affordable housing providers
- Federal Privacy Act