INTERNAL PRIVACY POLICY

Effective Date: 12/04/2017
Category: PRIVACY

Contact(s):
Nathan Prenzlow
CEO
712-262-3782
nprenzlow@spencerymca.org

This YMCA Internal Privacy Policy ("Privacy Policy") sets forth Spencer Family YMCA's policies and procedures for protecting the privacy of Personal Data, as defined below. The Privacy Policy is applicable to all Spencer Family YMCA employees.

1.0 DEFINITIONS

"Data Controllers" are those people that determine how and whether Personal Information is processed. Spencer Family YMCA is a Data Controller for purposes of these procedures. When we share information with YMCA of the USA, both organizations are Data Controllers.

"Data Processors" are those people that process Personal Information on behalf of a Data Controller.

"Data Subjects" are the people to whom the Personal Data relates.

"Personal Data" is any information about an identifiable individual. Examples of Personal Data include (but are not limited to)

- name, date of birth, and social security or other identity card number;
- contact information such as mailing address, email address, and phone numbers;
- credit card and financial account numbers;
- health or medical information;
- information contained in employee files, including employment history, evaluations, and information collected during the application and hiring process; and
- information related to employee benefits, such as the names of dependents, beneficiaries, and insurance policy information.

Properly anonymized and de-identified or aggregate data is not Personal Data.

"Process" is used very broadly to indicate performing any action on Personal Data, such as collecting, recording, organizing, storing, transferring, modifying, using, retaining, or deleting.

"Sensitive Personal Data" is Personal Data that relates to an identifiable person's health, finances, sexual orientation, religious beliefs, or criminal record.

2.0 PERSONAL DATA MINIMIZATION AND PRIVACY BY DESIGN

Privacy protection is integral to our YMCA's processing of Personal Data because it helps to protect our members and to let them feel comfortable sharing information with us, and this information helps us to grow and improve our community.

We collect and process Personal Data in a number of ways, including from the following:

- Members when they sign up to join this YMCA, including name, address, and payment information, or when they use various services and join difference groups and activities.
- Volunteers, employees, and applicants as part of their employment or application. This information may include job applications, employee records of training, documentation of performance appraisals, salary, and other employment records.
- Nonmember guests who visit for certain activities.

Such processes should be designed to minimize the unnecessary collection or use of Personal Data. For instance, use an identification number in place of a Social Security number when possible, and use a partial Social Security number in place of the full number when possible. Likewise, the use of anonymized and de-identified or aggregate data is generally preferable to the use of Personal Data.

3.0 PROCEDURES

All employees must comply with the following procedures:

3.1 Data Collection and Consent

Prior to the collection and processing of Personal Data, our YMCA must obtain consent from the Data Subject in a manner appropriate to the context. Most of the time, consent is implied from the circumstances. For instance, if members sign up for swim class, they expect the information to be used to organize the class and to communicate with them about the class, but they would not expect that information to be sold to local pizza chains for them to receive coupons. When Personal Data is used in ways that are not reasonably implied from the apparent circumstances, consent may be provided orally, in writing, or electronically, on an opt-in or opt-out basis generally, although uses of Sensitive Personal Data should have more clear opt-in consent.

Some people, such as children or persons with mental disabilities, may not be capable of providing personal consent to the collection, use, or disclosure of their own Personal Data. In those cases, we can rely upon the consent of those persons who are giving care to that person and who are entitled to consent on behalf of the individual in the given circumstances and in accordance with state and federal law. **Personal Data should not be collected from children without clear parental or legal guardian written consent, and Sensitive Personal Data collection requires particularly clear consent to collect.**

To provide notice and receive informed consent, disclose the following before collecting Personal Data when it is not otherwise clear from the circumstances:

- the identity of the person or entity that is collecting the Personal Data (i.e., the Data Controller);
- the purpose(s) for which the Personal Data is to be processed or used;
- the methods by which the Personal Data is to be collected;
- the scope of Personal Data that may be collected (e.g., types, over what time period, etc.); and
- the identity of anyone to whom the Personal Data may be disclosed or transferred.

The YMCA need not obtain consent from the Data Subject in the following limited circumstances:

- in an emergency that threatens an individual's life, health, or personal security;
- when the Personal Data is available and collected from a public source;
- when the processing is necessary for the performance of a contract to which the Data Subject is party, or in order to take steps at the request of the Data Subject prior to entering into a contract;
- when the processing is necessary for compliance with the YMCA's legal compliance obligations, such as to investigate and protect its legal interests;
- when the processing is necessary in order to protect the vital interests of the Data Subject, narrowly construed;
- in certain circumstances, when processing is necessary for the performance of a task carried out in the public interest;
- When processing is necessary for the YMCA's legitimate business interests, as disclosed to the Data Subject, consistent with the fundamental rights and freedoms of the Data Subject; or
- where the intended collection, use, processing, and/or disclosure is otherwise permitted or not precluded by applicable law.

3.2 Withdrawal of Consent

In some circumstances, consent to the collection and use of Personal Data may be withdrawn, subject to contractual and legal restrictions and reasonable notice. In general, our YMCA should allow and respect the withdrawal of consent to the greatest extent possible, such as with respect to the withdrawal of consent to receiving marketing materials or telephone calls.

Withdrawal of consent may have consequences, such as no longer being able to provide certain services or communicate in certain ways. In certain circumstances, consent may not be withdrawn with respect to certain necessary uses and disclosures of Personal Data, such as with respect to certain legal and contractual obligations.

Personal Data systems should be reasonably designed to allow for the effective withdrawal of consent. In particular, opt-out lists must be maintained, and communications must be scrubbed against these lists to be able to verify that recipients that they have expressed their wish not to receive are in fact, not receiving communications, even if they previously consented to receiving the communication. Compliance with such requests is particularly important with respect with any electronic and telecommunications (phone, fax, text, etc.) campaigns, consistent with the legal requirements applicable to the campaign. Awareness of the restrictions applicable to particular campaigns is the responsibility of the manager of that campaign, and it is their responsibility to consult with YMCA management and/or legal counsel in order to achieve full compliance in their specific circumstances.

3.3 Purpose Specification and Use Limitation

When Personal Data is used, our YMCA must use the Personal Data in a way that is compatible with the purposes for which it was collected, or for a reasonably related purpose. If Personal Data needs to be used for another purpose or handled in a way that the Data Subject has not provided consent, the YMCA should obtain the consent of the Data Subject for the new or different use.

Only YMCA personnel or third parties working on behalf of this YMCA with a legitimate business purpose may access or use Personal Data, and even those individuals may access such Personal Data only for legitimate purposes required by their positions. The more sensitive the Personal Data is, the greater the security should be to protect it.

3.4 Data Subject Access

Our YMCA should post a privacy notice so that Data Subjects can contact the appropriate person with inquiries or complaints regarding the use of their Personal Data. Our YMCA must make reasonable efforts to grant Data Subjects' requests to access their Personal Data. In accordance with these procedures, Data Subjects may ask the YMCA whether it maintains Personal Data about them, and the contents, if any, of that data. If the YMCA denies access, it should provide the Data Subject the reasons for such denial and allow the Data Subject to challenge the denial.

3.5 Data Accuracy

Our YMCA should use its best efforts to process accurate Personal Data. To this end, Data Subjects may make reasonable requests for the correction of any incorrect or misleading Personal Data about them. To the extent reasonably feasible, we must, as appropriate, correct or destroy Personal Data that is inaccurate, misleading, or out-of-date. If our YMCA does not make a requested correction, the request should be noted in the Data Subject's file to the extent feasible and explained to the Data Subject.

3.6 Data Retention

Our YMCA should not keep Personal Data longer than necessary for the purpose for which it was collected. Our YMCA must securely destroy or erase Personal Data from its systems when it is no longer required to accomplish the purpose for which it was collected. Our YMCA also should endeavor to ensure the secure deletion and destruction of Personal Data stored or maintained by third parties. We may, however, retain some Personal Data in order to comply with applicable laws, regulations, rules, and court orders.

3.7 Security

Our YMCA takes reasonable administrative, technical, and physical measures to safeguard against unauthorized processing or use of Personal Data, and against the accidental loss of, or damage to, Personal Data. These measures include:

- making available written plans to identify, prevent, detect, respond to, and recover from cybersecurity threats and incidents;
- developing security authentication procedures for accessing all systems that store Personal Data;
- maintaining patched, up-to-date anti-virus software, firewalls, and other computer security safeguards, and appointing appropriate personnel to be responsible for keeping such safeguards up-to-date;
- requiring third-party data processors, vendors and other service providers who will be processing Personal Data on behalf of this YMCA to maintain appropriate security measures;
- maintaining appropriate records of access to and processing of Personal Data;
- auditing Personal Data security at regular intervals (but no less than annually) and recording the results of such audits;
- using appropriate protections, such as encryption, to protect Sensitive Personal Data in transit and when stored on portable computer media as necessary or appropriate;
- utilizing appropriate and secure destruction methods of Personal Data as legally required; and
- taking all other reasonable measures as required from time to time by local laws and regulations.

3.8 Sharing Personal Data With Third Parties

The YMCA may share the Personal Data with its corporate affiliates, such as YMCA of the USA, and third parties that provide services to our YMCA to the extent such third parties are contractually required to follow the procedures set forth herein, or substantially equivalent standards, and to protect Personal Data in accordance with all relevant laws, regulations and

rules, and subject to any appropriate security measures and directions from our YMCA. These requirements should also apply to any subcontractors engaged by third parties.

Personal Data may not be sold, transferred, or disclosed to other third parties except as authorized in writing by YMCA management.

Prior to disclosing Personal Data to a third party, the YMCA may provide the Data Subject the opportunity to choose whether his or her information may be disclosed to that third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the Data Subject.

In all instances, Sensitive Personal Data should not be disclosed to unaffiliated third parties or used for new purposes without explicit consent or the presence of other circumstances requiring or justifying such use.

3.9 Confidentiality

Employees and third-party contractors may not disclose information made available on our YMCA's systems and networks, including to other YMCA personnel, except as expressly authorized by the appropriate manager. The duty of nondisclosure and confidentiality extends to interactions with third parties, including other employees, customers, business partners, and vendors.

3.10 Incident Reporting and Response

The suspected theft, loss, or unauthorized processing of data, including Personal Data, must be immediately addressed. Our YMCA must take steps to immediately investigate the cause of the security breach and make every effort to contain the breach. Our YMCA must follow the steps set forth in the Data Security Incident Response Plan when responding to security incidents.

3.11 Children's Information

If our YMCA intends to collect or use personal information from children under the age of 13, it must first obtain the verifiable consent of their parents or guardians, such as through consent forms that the parent or guardian signs in person. Consent need not be obtained where information about children is provided by their parents or guardians.

4.0 PRIVACY INQUIRIES AND DISPUTES

Our YMCA must designate an individual to handle complaints and disputes regarding the use of Personal Data. Our YMCA must inform the individuals from whom it collects Personal Data of a phone number or email address that they may contact for complaints or disputes about how their Personal Data is handled. These complaints and disputes shall be addressed by YMCA management, who may decide when consultation with legal counsel is appropriate in anticipation of potential litigation with the Data Subject. Internal processing of requests for legal counsel would be subject to attorney-client privilege and attorney work-product doctrine protections to the extent applicable under state or federal law. The person(s) authorized to handle complaints and disputes is CEO Nathan Prenzlow.

5.0 COMPLIANCE WITH AND MODIFICATION OF PROCEDURES

YMCA employees who violate this Privacy Policy may be subject to disciplinary actions, up to and including termination of employment.

As is appropriate, our YMCA may modify its procedures for the handling of Personal Data, but material changes to the handling of Personal Data cannot be applied retroactively without the express consent of the Data Subject unless consent was not necessary to collect and use the Personal Data.

To facilitate compliance with this Privacy Policy and to protect its workers, systems, information, and assets; our YMCA may review, audit, monitor, intercept, access, and disclose information processed or stored on YMCA equipment and technology, or on personally owned devices permitted YMCA network access.

If you become aware of any actual or suspected breach of this Policy, notify Nathan Prenzlow at 712-262-3782.

If you have any questions about this guidance, or for additional information or training, please contact us at 712-262-3782.

Our YMCA's management may monitor, assess, and promote compliance with this Policy by

- providing guidance regarding implementation of, and adherence to, the Policy;
- assisting with the design of initiatives to minimize the collection and other processing of Personal Data;
- designing and conducing appropriate privacy training;
- serving as an initial point of contact for privacy and Personal Data protection issues;
- handling privacy complaint investigations and resolutions;
- providing guidance regarding contracts for processing Personal Data;
- monitoring legal developments regarding privacy and data protection; and
- providing our YMCA with an ongoing assessment of compliance with applicable laws and industry best practices.

6.0 TRAINING

Employees with access to Personal Data shall receive annual training on this Privacy Policy.

7.0 REFERENCES

For questions related to the implementation of this Policy, contact Nathan Prenzlow at 712-262-3782.

Policy Revision History			
Version:	**Effective Date:**	**Authorized by:**	**Affected Provisions:**
Version 0.1	12/04/2017	**Nathan Prenzlow**	**--**