BOYS & GIRLS CLUBS
OF SILICON VALLEY

SAFETY HANDBOOK

LAST REVISED: APRIL 2025

Table of Contents:

OVERVIEW

The safety and protection of children and teens is the number one priority for Boys & Girls Clubs of Silicon Valley. Even one safety incident is too many. Any incident that impacts the well-being of the young people entrusted to our care is taken seriously.

With the goal of zero incidents, preventing accidents and incidents is critically important to the safety of our members. The Safety Handbook is designed to assist our Club to respond to incidents should they occur, with the goal to protect our members, staff, volunteers and the organization, and mitigate risk moving forward. There are several actions every Club site should take to prepare to respond to reported incidents.

If the incident involves an injury to a member, staff or volunteer, immediately take all necessary steps to ensure they are safe.

- Maintain and adhere to incident reporting protocols including reporting to authorities.
- Follow the board-approved Crisis Communications Plan.
- Follow the board-approved Emergency Operations Plan.
- Identify and contact incident response partners, when appropriate.

This Safety Handbook applies to all Boys & Girls Clubs of Silicon Valley employees and volunteers. All employees and volunteers must acknowledge and agree to abide by the statement(s) in the Safety Handbook.

Applicability

The Safety Handbook applies to all Boys & Girls Clubs of Silicon Valley employees, volunteers, vendors and any other person using or accessing Boys & Girls Clubs of Silicon Valley information or information systems. Exceptions to this policy must be approved by the CEO or his/her designated representative.

CHILD ABUSE PREVENTION POLICY

The priority of Boys & Girls Clubs of Silicon Valley is the physical and emotional safety of its members, staff and volunteers. Boys & Girls Clubs of Silicon Valley maintains a zero-tolerance policy for child abuse.

Boys & Girls Clubs of Silicon Valley implements policies and procedures for members, employees, volunteers, visitors or any victims of sexual abuse or misconduct to report any suspicion or allegation of abuse.

DEFINITIONS

One-on-One-Contact Prohibition: Boys & Girls Clubs of Silicon Valley prohibits isolated one-on-one interaction between Club participants and staff or volunteers, including board members. This includes prohibiting one-on-one contact at any time at the Club, in vehicles or by phone, text, social media or any other means.

Exceptions may only be made when delivering approved medical or counseling services by a licensed, trained therapist or similar professional according to professional guidelines. All staff and volunteers, including minor staff (under age 18), are strictly prohibited from meeting Club participants outside of any Club-sponsored activities. The only exception to this rule is if the Club participant is a child or sibling of a staff member or volunteer.

Child abuse is when an adult or another child, whether through action or by failing to act, causes serious emotional or physical harm to a child. Sexual abuse or misconduct may include but is not limited to:

- Any sexual activity, involvement or attempt of sexual contact with a person who is a minor (under 18 years old).
- Sexual activity with another who is legally incompetent.
- Physical assault or sexual violence, such as rape, statutory rape, abuse, molestation or any attempt to commit such acts.
- Unwanted and intentional physical conduct that is sexual in nature, such as touching, pinching, patting, brushing, massaging someone's neck or shoulders and/or pulling against another's body or clothes.
- Inappropriate activities, advances, comments, bullying, gestures, electronic communications or messages (e.g., by email, text, or social media).

Grooming is when someone builds an emotional connection with a child to gain their trust for the purposes of sexual abuse, sexual exploitation or trafficking. Grooming behaviors may include but are not limited to:

- Targeting specific youth for special attention, activities or gifts.
- Isolating youth from family members and friends physically or emotionally. This can include one-on-one interactions such as sleepovers, camping trips and day activities.
- Gradually crossing physical boundaries, full-frontal hugs, lap sitting or other "accidental" touches.

MANDATED REPORTING

All staff and volunteers are required annually to take BGCA's mandated training *Duty to Report: Mandated Reporter.* Every staff or volunteer of Boys & Girls Clubs of Silicon Valley who becomes aware of or has suspicion of child abuse or neglect must immediately report to Club leadership and Child Protective Services (CPS). Club staff are responsible for reporting the incident immediately to the appropriate authorities according to statewide mandated reporting laws, as well as to Boys & Girls Clubs of America (BGCA) within 24 hours via the critical incident system.

REQUIRED TRAINING

Boys & Girls Clubs of Silicon Valley conducts and reports through a BGCA-approved process. The following training for all staff and volunteers who have direct repetitive contact with young people (at the intervals noted for each).

Before providing services to young people, and annually thereafter:

1. BGCA-approved child abuse prevention courses
2. BGCA-approved mandated reporting courses
3. BGCA-approved grooming prevention courses
4. **Annually:** All company policies, including all safety policies specific to Boys & Girls Clubs of Silicon Valley and all non safety policies such as our Code of Ethics of Dress code policy.

PHYSICAL INTERACTIONS

Every staff member and volunteer of Boys & Girls Clubs of Silicon Valley is required to maintain appropriate physical contact with minors. Appropriate and prohibited interactions include but are not limited to the following:

Appropriate	Prohibited
● Side hugs ● Handshakes ● High-Fives and hand slapping ● Staff offers to holding hands with young children in escorting situations ○ Young children being defined as ages from TK-2nd grade, including any child with special needs/accommodations	● Full-frontal hugs or kisses ● Showing affection in isolated area ● Lap sitting ● Wrestling or piggyback/shoulder rides ● Tickling ● Allowing youth to cling to an adult's leg

VERBAL INTERACTIONS

Every staff member and volunteer of Boys & Girls Clubs of Silicon Valley is required to maintain appropriate verbal interactions with minors. Appropriate and prohibited interactions include but are not limited to the following:

Appropriate	Prohibited
● Positive reinforcement ● Child appropriate jokes (no adult content) ● Encouragement ● Praise	● Name calling ● Inappropriate jokes (adult content) ● Discussing personal issues or sexual encounters ● Secrets ● Profanity and derogatory remarks ● Harsh language that may frighten, threaten, or humiliate youth

ABUSE AND SAFETY RESOURCES

Boys & Girls Clubs of Silicon Valley prominently displays BGCA-approved collateral that shares ethics hotline, crisis text line and safety helpline information with members, staff, volunteers and families. We also share all safety policies with parents and guardians upon receiving a youth membership application. Boys & Girls Clubs of Silicon Valley is committed to providing a safe environment for members, staff and volunteers. To further ensure their safety, the organization prohibits all one-on-one interactions between Club members and staff and volunteers (including board members). Boys & Girls Clubs of Silicon Valley has an anonymous phone hotline that can be called 24/7 to report incidents (408) 317-2463.

All staff and volunteers must abide by the following:

- Ensure all meetings and communications between members and staff or volunteers are never private (see definition below).
- Ensure in-person meetings take place in areas where other staff and/or members are present.
- Communicate to another staff member whenever an emergency arises that necessitates an exception to this policy.
- Never initiate private or isolated one-on-one contact with a member.
- Never have a private or isolated meeting or communication with a member. This includes in-person meetings and virtual communications such as texting, video chat and social media between only a staff member or volunteer and a single member.
- Never transport one Club member at a time. This includes transportation in Club vehicles.

Exceptions may only be made when delivering medical or counseling services by a licensed, trained therapist or similar professional. All exceptions shall be documented and provided to Club leadership in advance. Club leadership must authorize the exception ahead of time.

If an emergency arises that necessitates an exception to this policy, the emergency exception shall be communicated to Club leadership as soon as practicable, and before engaging in one-on-one interaction.

PROHIBITION OF PRIVATE ONE-ONE INTERACTION POLICY

DEFINITION OF ONE-ON-ONE INTERACTION

One-on-one interaction is defined as any private contact or communication (including electronic communication) between any Club member and an adult, including adult staff, minor staff, volunteers, board members and others who might encounter members during regular programming and activities.

- Private contact/communication is any communication, in person or virtual, that is between one youth member and one adult (18 or over) that takes place in a secluded area, is not in plain sight and/or is done without the knowledge of others. Private places can include but are not limited to vehicles, rooms without visibility to others, private homes and hotel rooms. Examples of private contact include but are not limited to:
    - Meeting behind closed doors (in rooms without windows or visible sightlines) or any spaces that are not visible to others.
    - One staff transporting one member in a vehicle.
    - Electronic communications (text, video, social media, etc.) between one member and one staff or volunteer.

Public contact/communication is any communication or meeting, in person or virtual, that is between at least three individuals, including two staff and one member, one staff and two members or variations of these combinations. Examples of public contact include but are not limited to:

- Meeting in plain sight of others (e.g., in a quiet corner of an active games room).
- Transporting members via public transportation (bus, taxis, train, air, etc.) or transporting multiple members.
- Electronic communications with members (text, video, etc.) between multiple members and adults (e.g., group chats).
- Public places can include but are not limited to buses, airports, shopping malls, restaurants and schools.

IMPACT ON MENTORING PROGRAMS

Mentorship is a key component of Boys & Girls Club programming and has a tremendous positive impact on members. Prohibition of one-on-one interaction does not have to negatively affect mentor programs and/or relationship building. Mentors can adjust their practices to include:

- Holding mentor and coaching sessions in areas where other staff and/or members are present or can see you – for example, in large rooms where meetings are visible but not heard.
- Copying parents, staff or other members (when appropriate) on written and/or electronic communications.
- Scheduling meetings during Club hours and at the Club site.
- Documenting interactions between mentors and youth.

IMPACT ON PARTNERSHIPS WITH LOCAL MENTORING ORGANIZATIONS

- All local mentors are required to abide by Club policies.
- External mentors are required to abide by all Club safety policies and procedures.
- A written agreement should be in place to determine how and when the external organization assumes custody and responsibility of the member; these procedures should be clearly communicated to parents or guardians.
- Every interaction between mentor and youth will be documented and maintained.

IMPACT ON TRAVELING TO OFF-SITE EVENTS AND ACTIVITIES

- When traveling to external events such as Keystone, Youth of the Year or other off-site events, the one-on-one policy shall continue to be followed.
- Should the Club take responsibility for transporting members to and/or from an event, one staff member should not transport one single child at any time in a vehicle. Accommodations shall be made to ensure at least three people (two staff and one member or one staff and two members) are together when traveling. As an alternative, public transportation may be used (e.g., taxi, rideshares, public transport).
- If this arrangement presents staffing or budget challenges, consider the following:
    - Inviting parents or guardians to attend and/or chaperone their child. Including Additional Youth (e.g.,Junior Youth of the Year) and/or staff travel plans.
    - Coordinating with other Club houses or nearby organizations to travel together.
    - Traveling with additional staff or members.

- Parents and guardians should also provide written consent in each instance in which a member travels to any off-site event. NOTE: Parents or guardians are never allowed to provide consent for one-on-one interaction.
- These practices apply when coordinating field trips.

IMPACT ON TRANSPORTATION TO AND FROM THE CLUB

When transporting members to and/or from a Club-sponsored event or activity, single members should not be transported alone with one staff person. Consider the following to accommodate single children:

- Modify bus or van routes so single children aren't picked up first or dropped off last.
- Use a bus aid if available.
- Pick up and drop off children in groups.
- Modify staff schedules to ensure multiple staff are present.

EXCEPTIONS TO POLICY

Exceptions to the one-on-one policy can be made under the following circumstances:

- When delivering medical or counseling services by a licensed, trained therapist or similar professional (e.g., counselors, social workers).
- When the emotional or physical safety of a member is at risk and a private, one-on-one communication is deemed necessary by Club leadership.
- In emergency situations that could create a safety risk, exceptions can be made (e.g., if a member is not picked up by a parent and leaving them alone at the Club could be a safety risk).
- In these types of situations, staff must receive prior approval from Club leadership, and are required when transporting a member one-on-one.
    - Video recording required to be submitted to HR within 24 hours of transportation.

Should exceptions need to be made, the Club shall have policies in place to monitor interactions, including but not limited to:

- Disclosing the meeting to Club leadership and regularly checking in with the member and adult during conversations.
- Placing time limits on conversations.
- Meeting in rooms with clear sight lines (e.g., rooms with windows or glass doors).
- Documenting the interaction.
- In an emergency, disclosing the situation to another staff person before engaging in one-on-one interaction.

SUPERVISION & FACILITIES POLICY

SUPERVISION

Boys & Girls Clubs of Silicon Valley is committed to providing a safe environment. All Club activities and program spaces shall always be under continuous supervision by sight or sound (for restroom supervision) by an appropriate adult staff (18 or over). To ensure appropriate supervision, staff and volunteers:

- Must abide by the prohibition of private one-on-one interaction policy.
- Must abide by all the organization's disciplinary policies and procedures.
- Must ensure that at least one adult staff (18 and over) is present when supervising members.
- Must always maintain proper supervision ratios.
- Must be trained on appropriate supervision tactics and behavior patterns.
- Must ensure that all youth staff and volunteers are supervised by an adult (18 and over) staff member.
- Must immediately notify Club leadership and/or submit written reports detailing supervision issues, accidents or critical incidents.
- Must never use electronic devices such as cell phones, PDAs or other communication devices while supervising members unless for Club purposes, as defined in the Acceptable Technology Use Policy.

RESTROOM USAGE

Boys & Girls Clubs of Silicon Valley is committed to providing a safe, clean environment and enforces the following restroom policy for members, staff, volunteers and other adults.

- There will be either a designated adult restroom or procedures to ensure adults and minors never utilize a restroom at the same time.
- The Club will either have single-user restrooms or multi-user restrooms with single stalls that can be secured from the inside.
- When using restrooms at public facilities during field trips, a minimum of three youth will be escorted by one staff member, who will wait outside the main entrance of the restroom.

RESTROOM MONITORING

Restrooms shall be regularly monitored by designated staff according to a schedule set by Club leadership. Monitoring includes walk-throughs, inspections and/or any (but not necessarily all) of the best practices outlined below:

- Implementing procedures to limit the number of children using restrooms at the same time.
- Prohibiting younger children and teens from sharing a restroom.
- Positioning staff near restroom entries to maintain auditory supervision of space.
- Designing or renovating multi-user restrooms to eliminate outer doors, while maintaining privacy with individual stalls.

Staff observing unacceptable restroom conditions or incidents shall:

- Immediately notify Club leadership of the incident.
- Document, in writing, restroom conduct incidents and report them to Club leadership as soon as possible in compliance with the Club's Incident Reporting Policy.

SHARED-USE RESTROOMS

- On a field trip or when using a public restroom, youth shall never enter the restroom alone unless it is a single-stall restroom that is empty.
- Youth shall follow the "rule of three" in using public restrooms, with at least two youth and an adult walking to the restrooms and three youth entering a multi-stall facility together. The adult will remain outside the restroom door to provide auditory surveillance.
- Whenever possible, staff/volunteers will monitor and clear public restrooms before use by members to ensure that the facility is free of adults – and clear of youth not involved in the Club program – before allowing youth to use the facilities. Alternatively, staff members will stand in the restroom doorway and/or hold the door at least partially open when supervising member use of public restrooms. Staff may position themselves inside the restroom near the sinks if positioning at the door is not feasible or is deemed ineffective.
- In a shared-use facility, Boys & Girls Clubs staff will utilize the best practice of shutting the exterior door to the restroom and using an "Occupied" sign outside of the door to alert others that they must wait until Club members have exited the restroom before they can enter.

ENTRANCE AND EXIT CONTROL

All facility entries and exits shall be locked, controlled and monitored by paid adult staff (18 or over) during all hours of operation, along with a system to monitor and track everyone who is in the facility.

All exit doors shall have an audible alarm to discourage unauthorized use to exit or enter the facility.

Only designated adult staff (18 or over) shall be authorized to possess keys and/or badges to open any facility. If an employee is supervising a scheduled activity, they shall be responsible for the security of their program space.

FACILITY CONDITION

All program spaces shall have clear lines of visibility and be monitored by adult staff when in use. Areas that are not in use shall remain locked and only accessible by adult staff.

All interior and exterior spaces, hallways, stairs and stairways shall be monitored, maintained, well-lit, clean and free of hazards and obstructions. All storage closets and other unused spaces are to be locked during operational hours.

Damages to facilities shall be repaired in a reasonable manner. Damages that pose imminent risk to the health and safety of members, staff or volunteers shall be repaired immediately. If immediate repair to damage that poses imminent risk is not possible, Club leadership shall determine whether temporary or permanent closure of the facility may be required. Any damage to a facility that results in an incident deemed critical to the organization shall be reported to the appropriate authorities as a critical incident.

FOOD AND DRINK

Any distribution, preparation or consumption of food and/or drink at any facility shall comply with all applicable food services sanitation and public health codes. If food is prepared and served on site, required city or county health department inspection certificates shall be posted. Any dangerous kitchen utensils, including knives, shall be properly and securely stored.

SCREENING AND ONBOARDING

Boys & Girls Clubs of Silicon Valley is committed to selecting and retaining effective staff and volunteers to serve our youth. As part of the selection process and in accordance with state background check regulations, background checks and screening procedures are conducted in accordance with this policy.

BACKGROUND CHECKS

Boys & Girls Clubs of Silicon Valley conducts criminal background checks of all employees, including minors; board volunteers and others who serve on a standing committee; and all other volunteers, including partners and minors, who have direct repetitive contact with minors. These checks will be conducted prior to employment and engaging with members.

Name-based or fingerprint-based record searches may be used in any combination, but the background check shall at a minimum:

- Verify the person's identity and legal aliases through verification of a social security number.
- Provide a national Sex Offender Registry search.
- Provide a comprehensive criminal search that includes a national search.
- Provide a comprehensive local criminal search that includes either a statewide or county level criminal search, depending on jurisdiction *(a current list of jurisdictions can be found at www.bgca.net/childsafety)*.
- Include any additional background check criteria required by organizational policies, funding or licensing agencies or required in the applicable jurisdiction, such as motor vehicle records or child abuse registry.

All background check findings shall be considered when making employment or volunteer decisions, and Boys & Girls Clubs of Silicon Valley will not employ potential staff or engage potential volunteers if such individual:

- Refuses to consent to a criminal background check.
- Makes a false statement in connection with such criminal background check.
- Is registered, or is required to be registered, on a state or national sex offender registry.
- Has been convicted of a felony consisting of:
    1. Murder
    2. Child abuse
    3. Domestic violence

4. Abduction or human trafficking
5. A crime involving rape or sexual assault
6. Arson
7. Weapons
8. Physical assault or battery
9. Drug possession, use or distribution in the last five years

- Has been convicted of any misdemeanor or felony against children, including child pornography.

INTERVIEWING

Boys & Girls Clubs of Silicon Valley will conduct behavioral-based interviews with every candidate for employment or volunteer service using BGCA provided behavioral-based interview questions.

REFERENCE CHECKS

Boys & Girls Clubs of Silicon Valley conducts reference checks on any candidate for employment or volunteer with direct repetitive contact with young people. Should candidates for employment have previous experience with a Boys & Girls Club, information on the candidate's eligibility for rehire/volunteering must be obtained from all previous Boys & Girls Clubs for which the candidate worked prior to extending an offer for employment or volunteer service. Additionally, Boys & Girls Clubs of Silicon Valley provides reference materials when asked by other member organizations.

STAFF AND VOLUNTEER ONBOARDING

Upon offer of a position, each new Club employee shall receive and confirm in writing receipt of an up-to date employee handbook that, at a minimum, articulates current:

- Conditions of employment;
- Benefits;
- Rights and responsibilities of employees;
- Club safety policies; and
- Any other important employment-related information.

Before working with any Club members, all staff and volunteers at a minimum shall be given an orientation that includes an overview of the following:

- The organization's mission, goals, policies and procedures and schedule
- Job descriptions and performance standards for their position

- The needs and other relevant characteristics of program participants, including cultural and socioeconomic characteristics
- Personnel and volunteer policies and procedures, including expectations regarding work hours and schedules, breaks and planning time
- Operational policies and procedures related to safety, supervision, transportation, facilities,emergency operations, etc.
- Completion of the all required **Child Abuse Prevention Trainings** approved by BGCA.

DRUG AND ALCOHOL FREE WORKPLACE POLICY

DRUG AND ALCOHOL POLICY

Boys & Girls Clubs of Silicon Valley is committed to providing a safe environment for members, staff and volunteers. To further ensure their safety, the organization maintains a drug- and alcohol-free workplace. The unlawful or improper use of drugs – including marijuana, controlled substances, prescription drugs, or alcohol in the workplace – presents a danger to everyone. The organization also has a duty to comply with the requirements of the Drug-Free Workplace Act of 1988.

- Employees are prohibited from reporting to work or working while under the influence of alcohol and/or illegal or unauthorized drugs.
- Employees are prohibited from reporting to work or working when the employee is using any legal drugs; exceptions can be made in accordance with state law when the use is pursuant to a doctor's orders and the doctor has advised the employee that the substance does not adversely affect the employee's ability to safely perform his or her job duties.
    - Employees taking any legal drugs that potentially affect job safety or performance are responsible for notifying their supervisor and/or Club leadership so that a determination of job performance or a reasonable accommodation can be made. An employee may not be permitted to perform their job duties unless such a determination or reasonable accommodation has been made.
- Employees are prohibited from engaging in the unlawful or unauthorized manufacturing, distribution, dispensing, sale or possession of illegal drugs and alcohol in the workplace, including on organization paid time, on organization premises, in organization vehicles or while engaged in organization activities.
- Employees must notify their supervisor and/or Club leadership immediately of any criminal drug or alcohol violation.
- Employment with the organization is conditional upon full compliance with the foregoing drug and alcohol free workplace policy. Any violation of this policy might result in disciplinary action, up to and including termination.

Boys & Girls Clubs of Silicon Valley further reserves the right to take any and all appropriate and lawful actions necessary to enforce this drug and alcohol free workplace policy, including but not limited to the inspection of organization-issued lockers, desks or other suspected areas of

concealment, as well as an employee's personal property when the organization has reasonable suspicion to believe that the employee has violated this policy.

SMOKING POLICY

Boys & Girls Clubs of Silicon Valley will comply with all applicable federal, state and local regulations regarding non-smoking in the workplace in order to provide a work environment that promotes productivity and the well-being of its employees. Smoking in the workplace can adversely affect members, employees and volunteers and is restricted at all facilities.

Smoking is prohibited at all Boys & Girls Clubs properties. The smoking policy applies to employees, volunteers, and members while on Club premises or during Club activities (on or off site).

Smoking is defined to include the use of any tobacco-containing products, including cigarettes, cigars and pipes, as well as the use of electronic cigarettes (e-cigarettes), and vaporizers.

REASONABLE SUSPICION

Staff and or volunteers shall immediately notify Club leadership of any action by an employee or volunteer who demonstrates an unusual pattern of behavior suggesting that they are under the influence of drugs or alcohol. Club leadership will determine whether the employee should be examined by a physician or clinic and/or tested for drugs or alcohol in accordance with the Club's drug-testing policies below. Employees and volunteers believed to be under the influence of drugs or alcohol will be required to leave the premises. Any illegal drugs or drug paraphernalia will be turned over to the appropriate law enforcement agency and may result in criminal prosecution.

Examples of behavior suggesting that employees or volunteers are under the influence of drugs or alcohol include but are not limited to:

- Odors (smell of alcohol, body odor or urine);
- Movements (unsteady, fidgety, dizzy);
- Eyes (dilated, constricted or watery eyes or involuntary eye movements);
- Face (flushed, sweating, confused or blank look);
- Speech (slurred, slow, distracted mid-thought, inability to verbalize thoughts);
- Emotions (argumentative, agitated, irritable, drowsy);
- Actions (yawning, twitching); or
- Inactions (sleeping, unconscious, no reaction to questions).

- Unusual patterns of behavior that may suggest drug or alcohol misuse include but are not limited to:
    - Repeatedly calling in sick
    - Being absent directly before or after holidays and weekends
    - Repeatedly damaging inventory or failing to meet reasonable work schedules
    - Being involved in frequent accidents that can be related to the use of drugs or other substances

INSPECTION AND TESTING

Boys & Girls Clubs of Silicon Valley reserves the right to take any and all appropriate and lawful actions necessary to enforce this drug and alcohol free workplace policy, including but not limited to the inspection of organization-issued lockers, desks or other suspected areas of concealment, as well as an employee's personal property when the organization has reasonable suspicion to believe that the employee has violated this drug and alcohol free workplace policy (see “Reasonable Suspicion” above).

Screening, testing and security measures may be used as methods of enforcement, as permitted by applicable state law. It is a violation of this policy to refuse to submit to testing. Tests that are paid for by the organization are the property of the organization, and the examination records will be treated as confidential and held in separate medical files. However, records of specific examinations will be made available, if required by law or regulation, to the employee, persons designated and authorized by the employee, public agencies, relevant insurance companies and/or the employee’s doctor.

PRESCRIPTION MEDICATION AND LEGAL DRUGS

Employees and volunteers are prohibited from reporting to work or working when using any legal drugs, except when the use is pursuant to a doctor’s orders and the doctor has advised the employee or volunteer that the substance does not adversely affect the employee’s or volunteer’s ability to safely perform his or her duties.

Employees and volunteers taking a legal drug, such as prescription medication or medical marijuana, that potentially affects job safety or performance are responsible for notifying their supervisor and/or Club leadership so that a determination of job performance or reasonable accommodation can be made. An employee/volunteer may not be permitted to perform their job duties unless such a determination or reasonable accommodation is made. Clear reporting policies and procedures are an important element in responding to incidents that might occur in

Clubhouses. Staff and volunteers must at a minimum immediately report and document all safety incidents that might affect staff, volunteers, members and others who visit Clubhouses.

INCIDENT MANAGEMENT POLICY

GENERAL INCIDENT DESCRIPTION

Safety incidents can include but are not limited to:

- Inappropriate activity between adults (18 and over) and youth
- Inappropriate activity between multiple youth
- Allegations of abuse
- Bullying behavior
- Inappropriate electronic communications between adults (18 or over) and youth
- Minor and major medical emergencies
- Accidents, including slips and falls
- Threats made by or against staff, volunteers and/or members
- Physical assaults and injuries, including fights
- Missing children
- Criminal activity, including theft and robbery
- Other incidents as deemed appropriate by Club leadership.

Safety incidents include those that occur during Club programs, on Club premises and/or during a Club affiliated program or trip.

INTERNAL INCIDENT REPORTING

Any employee or volunteer who becomes aware of an incident, as defined in this policy, shall immediately complete an incident report and submit the incident to Club leadership.
The following information shall be included on an Incident Report:

- Date, Club site name, and address, city, and zip code
- Incident details (if applicable)
- Witnesses and contact information
- Names of all involved (youth and staff if applicable)
- All notifications made (first responders, parents, leadership, etc.)
- Supporting documents if applicable (videos or photos)

EXTERNAL INCIDENT REPORTING

Boys & Girls Clubs of Silicon Valley follows all applicable mandated reporting statutes and regulations and all applicable federal, state and local laws (including those around licensing, for licensed organizations) for the protection and safety of youth. Types of incidents reported include but are not limited to:

- Inappropriate activity between adults (18 or over) and youth;
- Inappropriate activity between multiple youth;
- Allegations of child abuse;
- Any form of child pornography;
- Criminal activity, including assault, theft and robbery; or
- Children missing from the premises.
- Self harm and/or threatening to self-harm

INCIDENT INVESTIGATION

Boys & Girls Clubs of Silicon Valley takes all incidents seriously and is committed to supporting external investigations of all reported incidents and allegations or internal investigations by the Safety Committee when not an externally reportable incident.

Federal, state and local criminal and or mandated child abuse reporting laws must be complied with before any consideration of an internal investigation. The internal investigation should never be viewed as a substitute for a required criminal or child protective services investigation. In the event that an incident involves an allegation against a staff member, volunteer or Club member, the Club shall suspend that individual immediately (employees with pay) and maintain the suspension throughout the course of the investigation.

BGCA CRITICAL INCIDENT REPORTING

Each member organization shall immediately report any allegation of abuse or potential criminal matter to law enforcement. In addition, each member organization shall report the following critical incidents to BGCA within 24 hours:

- Any instance or allegation of child abuse, including physical, emotional or sexual abuse; sexual misconduct or exploitation (Club-related or not) against any child by a current employee or volunteer; or any Club-related instance by a former employee or volunteer.
- Any instance or allegation of child abuse, including physical, emotional or sexual abuse; or sexual misconduct or exploitation by a youth towards another youth at a Club site or during a Club- sponsored activity.

- Any child who might have been abducted or reported missing from a Club site or Club-sponsored activity.
- Any major medical emergency involving a child, staff member or volunteer at a Club site or during a Club-sponsored activity leading to extended hospitalization, permanent injury or death; or a mental health crisis with a child requiring outside care.
- Any instance or allegation of abuse, including physical, emotional or sexual abuse, sexual misconduct, harassment or exploitation (Club-related or not) involving any staff member; or any Club-related instance or allegation of abuse, including physical, emotional or sexual abuse, sexual misconduct harassment or exploitation against a volunteer or visitor.
- Any failure to comply with requirements set forth by child care licensing agencies or organizations.
- Any known or suspected felony-level criminal act committed at a Club site or during a Club- sponsored activity.
- Any misappropriation of organizational funds or any amount of federal funds.
- Any criminal or civil legal action involving the organization, its employees or volunteers, as well as any changes in the status of an open organization-related legal action.
- Negative media attention that could compromise the reputation of the member organization or Boys & Girls Clubs of America brand.
- Any other incident deemed critical by the organization.

Failure to report safety incidents to Boys & Girls Clubs of America could result in a funding hold or the organization being placed on provisional status.

DATA AND CYBER SECURITY POLICY

PURPOSE

Boys & Girls Clubs of Silicon Valley Data and Cyber Security Policy is the foundation of the organization's Information Security Program. Information security is a significant aspect of managerial decision making and facilitates secure business operations. These policies enable the IT team to securely manage information assets, maintain accountability, and provide the security framework upon which subsequent security efforts will be based to define appropriate management of all information assets.

Boys & Girls Clubs of Silicon Valley Data and Cyber Security Policy applies to all staff, volunteers, and partners utilizing Boys & Girls Clubs of Silicon Valley assets. Policies are intended to manage the confidentiality, integrity and availability of information assets and are defined as any information system (hardware or software), data, networks and components owned or leased by Boys & Girls Clubs of Silicon Valley or its designated representatives.

GENERAL

- All staff, volunteers, and or other authorized persons using or accessing Boys & Girls Clubs of Silicon Valley information or information systems must adhere to the following policies:
    - General Security Policy
    - System Security Policy
    - Desktop Service Security Policy
    - Internet Acceptable Use Policy
    - Social Media Policy
    - Personal Equipment Policy
    - Virus, Hostile and Malicious Code Policy
- All information systems within Boys & Girls Clubs of Silicon Valley are the property of Boys & Girls Clubs of Silicon Valley and will be used in compliance with appropriate policy guidelines.
- Information placed on Boys & Girls Clubs of Silicon Valley information system resources becomes the property of Boys & Girls Clubs of Silicon Valley.
- Circumvention of Boys & Girls Clubs of Silicon Valley security policies and procedures (i.e., disconnecting or tunneling a protocol through a firewall) is strictly prohibited.

- Unauthorized use, destruction, modification and/or distribution of Boys & Girls Clubs of Silicon Valley information or information systems is prohibited.
- All users will acknowledge understanding and acceptance by signing the appropriate Boys & Girls Clubs of Silicon Valley policy statements prior to use of information assets or systems.
- All users will report any irregularities or suspicious occurrences found in information or information systems to the IT team at support@npce.com immediately upon detection.
- Boys & Girls Clubs of Silicon Valley information systems and information will be subject to monitoring at all times. Use of Boys & Girls Clubs of Silicon Valley information systems constitutes acceptance of this monitoring policy.
- Use of any Boys & Girls Clubs of Silicon Valley information system or dissemination of information in a manner bringing disrepute, damage or ill will against Boys & Girls Clubs of Silicon Valley is not authorized.
- Release of Boys & Girls Clubs of Silicon Valley information will be in accordance with Boys & Girls Clubs of Silicon Valley Policy Statements.
- Users will not attach their own computer or test equipment to Boys & Girls Clubs of Silicon Valley computers or networks without prior approval of the IT team or its designated representative.
- Only licensed and approved software will be used on any organizational computing resource.
- All devices assigned to Boys & Girls Clubs of Silicon Valley employees are property of the organization. All part time employees assigned a club device must leave the device at Boys and Girls Clubs of Silicon Valley facility, loaded in a club storage locker while not in use, and are not allowed to take the device home for personal use.
- All licensed software will be write-protected and stored by the IT team.
- Boys & Girls Clubs of Silicon Valley users will scan all files introduced into its environment for virus, hostile and malicious code before use.
- The IT team will ensure that Boys & Girls Clubs of Silicon Valley obtains, deploys, and regularly provides the latest in virus protection and detection tools.
- All information systems media, including disks, CDs and Universal Serial Bus (USB) drives, introduced to Boys & Girls Clubs of Silicon Valley environment will be scanned for virus, hostile and malicious code.
- All email will be scanned for virus, hostile and malicious code.
- All internet file transfers will be scanned for virus, hostile and malicious code.
- The unauthorized development, transfer or execution for virus, hostile and malicious code is strictly prohibited.

SYSTEM SECURITY

Boys & Girls Clubs of Silicon Valley's System Security Policy addresses access control, use of hardware, operating systems, software, servers and backup requirements for all systems maintained and operated by Boys & Girls Clubs of Silicon Valley.

PASSWORD SYSTEM SECURITY

Because poorly selected, reusable passwords represent the most vulnerable aspects of information security, Boys & Girls Clubs of Silicon Valley has adopted thorough policies to ensure the private information of our members and our proprietary organizational data are kept secure. Strong password practices help safeguard BGCSV systems, networks, and data from unauthorized access.

- Passwords will conform to the following criteria:
    - Passwords will be a minimum of 12 characters
    - Passwords must consist of at least one uppercase letter, one lowercase letter and one number.
- Passwords must not contain:
    - Sequential characters (e.g., "12345", "abcdef")
    - Keyboard patterns (e.g., "qwerty", "asdfgh")
    - Personal information (e.g., name, birthday, address, pet's name)
    - Parts of usernames or login IDs
- Passwords must be changed at least every 6 months
- Passwords used previously must not be reused
- Any suspicious queries regarding passwords will be reported to the IT team at support@npce.com.
- Passwords will be protected as Boys & Girls Clubs of Silicon Valley proprietary information.
- Users will be forced to unlock their computers using their network password after 60 minutes of inactivity on their desktops.
- All system passwords will be changed within 24 hours after a possible compromise as determined by IT.
- When users leave the organization, their accounts will be immediately disabled or deleted.
- If the user leaving the organization was a privileged user or a network administrator, all system passwords will be changed immediately.

CONFIDENTIALITY

Passwords should be considered confidential data and treated with the same discretion as any of the organization's proprietary information. The following guidelines apply to the confidentiality of passwords used by the Club's employees:

To maintain the confidentiality and security of user credentials:

- Passwords must be treated as confidential and proprietary information
- Users must not share passwords with anyone, including co-workers, supervisors, IT vendors (e.g., NPCE), or family members
- Passwords must not be reused across different systems or accounts
- Passwords must not be written down or stored in unsecured locations—this includes both physical (e.g., sticky notes) and digital (e.g., spreadsheets) formats
- Passwords must not be transmitted via email, chat, or phone calls
- If a password compromise is suspected:
    - Immediately change the password
    - Open a ticket to report the incident to IT
    - Secure any affected accounts

DESKTOP SERVICES SECURITY

Boys & Girls Clubs of Silicon Valley Desktop Services Security Policy addresses the authorized and legitimate use of hardware, operating systems, software, LAN, file servers and all other peripherals used to access any Boys & Girls Clubs of Silicon Valley information system:

- Only system administrators will have the ability to install software.
- Unauthorized copying or distributing of copyrighted software is a violation of Federal Copyright Law and will not be permitted.
- Personal software will not be installed on any Boys & Girls Clubs of Silicon Valley machine.
- Users will not allow non-employees to use Boys & Girls Clubs of Silicon Valley machines or devices without authorization of the IT team.
- The following items are organization policy for security monitoring:
    - All Boys & Girls Clubs of Silicon Valley systems and network activities will be subject to monitoring. Use of Boys & Girls Clubs of Silicon Valley systems and networks constitutes consent to this monitoring.
    - Disabling or interfering with virus protection software is prohibited.
    - Disabling or interfering with logging, auditing, or monitoring software is prohibited.
    - All Boys & Girls Clubs of Silicon Valley desktop services will be subject to inventory and inspection.

- Security irregularities, incidents, or emergencies related to Boys & Girls Clubs of Silicon Valley information or system will be reported to the IT team immediately.
- Sabotage, destruction, misuse, or unauthorized repairs are prohibited on Boys & Girls Clubs of Silicon Valley information systems.
- Desktop resources will not be used to compromise, harm, destroy or modify any other service or resource on Boys & Girls Clubs of Silicon Valley information system.
- All data on information systems at Boys & Girls Clubs of Silicon Valley is classified as organizational proprietary information.
- Users will secure all printed material and other electronic media associated with their use of Boys & Girls Clubs of Silicon Valley information and information systems.
- Storage, development, or the unauthorized use of tools that compromise security (such as password crackers or network sniffers) are prohibited.

INTERNET ACCEPTABLE USE

Internet access is provided to Boys & Girls Clubs of Silicon Valley employees to conduct Boys & Girls Clubs of Silicon Valley business. While these resources are to be used primarily for Boys & Girls Clubs of Silicon Valley business, the organization realizes that employees may occasionally use them for personal matters and therefore provides access to appropriate personal sites during non-business hours:

- Non-business internet activity will be restricted to non-business hours. Boys & Girls Clubs of Silicon Valley may actively block non-business sites during business hours.
- The definition of non-business sites is the sole discretion of the IT team. This definition can, and will, change without notice as the internet evolves.
- Internet activity will be monitored for misuse.
- Internet activities that can be attributed to a Boys & Girls Clubs of Silicon Valley domain address (such as posting to newsgroups, use of chat facilities and participation in mail lists) must not bring disrepute to Boys & Girls Clubs of Silicon Valley or associate Boys & Girls Clubs of Silicon Valley with issues outside the core mission and focus of the organization. Any statements representing the organization's official position must be approved in writing before being shared publicly.
- Internet use must not have a negative effect on Boys & Girls Clubs of Silicon Valley operations.
- Users will not make unauthorized purchases or business commitments through the internet.
- Internet services will not be used for personal gain or outside business ventures.

- Internet users will make full attribution of sources for materials collected from the internet. Plagiarism or violation of copyright is prohibited.
- Release of Boys & Girls Clubs of Silicon Valley proprietary information to the internet (i.e., posting information to a newsgroup) is prohibited.
- All internet users will immediately notify the IT team (support@npce.com) of any suspicious activity.
- Remote access to Boys & Girls Clubs of Silicon Valley internal network through the internet will be encrypted and authenticated in a manner authorized by the IT team.
- Accessing personal social networking accounts (including but not limited to Facebook, Instagram, Twitter, LinkedIn) or using Boys & Girls Clubs of Silicon Valley email for social networking purposes is prohibited. The use of social networking sites for specific business purposes must be pre-approved or assigned by a manager/supervisor.

EMAIL SECURITY POLICY

Boys & Girls Clubs of Silicon Valley Email Security Policy specifies mechanisms for the protection of information sent or retrieved through email. In addition, the policy guides staff and volunteers of Boys & Girls Clubs of Silicon Valley in the acceptable use of email. For this policy, email is described as any computer-based messaging including notes, memos, letters and data files that may be sent as attachments. Staff and volunteers are responsible for exercising due diligence for the protection of information sent or retrieved through email.

ACCESS CONTROLS

- All email on Boys & Girls Clubs of Silicon Valley information systems, including personal email, is the property of Boys & Girls Clubs of Silicon Valley. As such, email may be periodically monitored for compliance with this policy.
- Individual email accounts are intended to be used only by the person to whom they are assigned. Special arrangements can be made to share information between team members. In all other cases, no user is authorized to open or read the email of another without the express consent of senior management (i.e. CEO or Head of HR).
- Email is provided to the users of Boys & Girls Clubs of Silicon Valley primarily to enhance their ability to conduct Boys & Girls Clubs of Silicon Valley business.
- Mailbox is defined as the combined total of deleted items, inbox, sent items and any user-created email folders. Users will receive a warning message stating that they need to clear out space when their mailbox size reaches 50GB. However, users will continue to receive incoming messages.
- Terminated employees will have all email access immediately blocked.

- Users who leave the company will have all new emails automatically forwarded to their supervisor, or their designated representative, for 30 days as determined by the supervisor.
- The former employee's supervisor is responsible for disseminating stored emails to the appropriate party. Thirty days after the date of termination, the former employee's mailbox will be permanently removed from the system.

CONTENT

- Use of profane, inappropriate, pornographic, slanderous or misleading content in email is prohibited.
- Use of email to spam (i.e., global send, mail barrage) is prohibited. This includes the forwarding of chain emails.
- Use of email to communicate sexual or other harassment is prohibited. Users may not include any words or phrases that may be construed as derogatory based on race, color, sex, age, disability, national origin or any other category.
- Use of email to send unprofessional or derogatory messages is prohibited.
- Forging of email content (i.e., identification, addresses) is prohibited.
- All outgoing email will automatically include the following statement as part of the user's email signature: "This email is intended solely for the person or entity to which it is addressed and may contain confidential and/or privileged information. Any review, dissemination, copying, printing or other use of this email by persons or entities other than the addressee is prohibited. If you have received this email in error, please contact the sender immediately, and delete the material from your computer."

USAGE

- Any email activity that is in violation of policy statements or that constitutes suspicious or threatening internal or external activity will be reported.
- When sending email, users should verify all recipients to whom they are sending the message(s).
- Be aware that deleting an email message does not necessarily mean it has been deleted from the system.
- Do not click on any suspicious emails and all phishing emails should be forwarded to IT at support@npce.com, for blocking and banning purposes.

ONLINE SOCIAL NETWORKING

Boys & Girls Clubs of Silicon Valley is committed to maintaining a good relationship with employees and with the public. The way the public views Boys & Girls Clubs of Silicon Valley is

vital to promoting our brand, serving our members, retaining first-class employees, recruiting new employees, and marketing our services.

While Boys & Girls Clubs of Silicon Valley has no intentions of controlling employees' actions outside of work, it is important that employees practice caution and use discretion when posting content on the internet, especially on social networking sites that could affect Boys & Girls Clubs of Silicon Valley 's operations or reputation. This policy serves as a notice on the practice of social networking for all employees to read and understand.

The following is the purpose of the Online Social Networking Policy:

- To maintain a constructive relationship between the organization and its employees.
- To reduce the possibility of risk to Boys & Girls Clubs of Silicon Valley or its reputation.
- To discourage the use of company time for personal networking.
- To ensure employees are aware of their actions while engaging in social networking, the number of individuals who can access information presented on social networking sites and the consequences associated with these actions.

Definitions

Social Networking is any activity that involves interaction in online communities of people. This interaction includes, but is not limited to, browsing other users' profiles, browsing other users' photos, reading messages sent through social networking forums and engaging in online communities' instant messaging services.

Social Networking Sites is specific online communities of users, or any website that links individuals electronically and provides a forum where users can connect and share information. These websites can be general or tailored to specific interests or certain types of users. Examples of popular social networking sites include Facebook, Instagram, Twitter, and LinkedIn. The list of domains that constitute social networking sites is ever-growing and changing because of the nature of the internet.

Social Networking Profile is a specific user's personalized webpage within a certain social networking site, usually containing personal information such as one's name, birthday, profile photo and interests.

Microblogging is the practice of publishing your recent whereabouts, thoughts or activities on a social networking site for other users to see. This is the main focus of social networking sites such as Twitter, but it also includes features like status updates like on Facebook and is prohibited from accessing on Boys & Girls Clubs of Silicon Valley computers and during work hours.

Business Purposes Using a social networking site for the organization's gain, usually as a task or assignment given by a manager or supervisor. This can be done either through a specific

company account on a given social networking site or through a personal account for the purposes of recruiting or marketing for Boys & Girls Clubs of Silicon Valley.

Prohibited Use It is important that employees use their time while at work to conduct the organization's business. Unless specifically required to perform the duties of your job, employees are prohibited from accessing social networking sites on Boys & Girls Clubs of Silicon Valley computers and during work hours.

PERSONAL EQUIPMENT POLICY

This policy provides guidelines for using corporate IT support resources for personally owned equipment and related software including, but not limited to: notebook computers, desktop computers, personal digital assistants (PDAs), smartphones and cell phones.

Boys & Girls Clubs of Silicon Valley recognizes that personally owned equipment can play a valuable role in convenience, efficiency and productivity of its employees. Nonetheless, the use of corporate resources, human or otherwise, for personal gain must be monitored closely.

As a general rule, employees of Boys & Girls Clubs of Silicon Valley will not use or request corporate IT resources in the use, network connectivity or installation of their personally owned equipment or software.

Personally-owned notebooks and desktop computers will not be granted direct physical access to the network. Employees seeking to access Boys & Girls Clubs of Silicon Valley network from a remote location using their personally owned computer may do so using only Boys & Girls Clubs of Silicon Valley authorized software and only with the approval of the employee's supervisor or manager.

PDAs and smartphones, which include devices using iPhone, Google, Samsung, and Android technologies, will be supported according the following rules:

- Employees are responsible for learning, administering, installing and setting up their own PDAs or smartphones.
- Corporate IT resources should not be used for assistance in the basic operation of these devices.
- Upon request, the IT team will install the necessary synchronization software to the employee's desktop or notebook computer.

VIRUS, HOSTILE, AND MALICIOUS CODE SECURITY

The intent of this policy is to better protect Boys & Girls Clubs of Silicon Valley assets against attack from destructive or malicious programs:

- Any public domain, freeware or shareware software will be evaluated by the IT team prior to installation on any company resource.
- No unauthorized software will be downloaded and installed on end user machines without express approval from the IT team.
- System users will not execute programs of unknown origin, as they may contain malicious logic.

TECHNOLOGY ACCEPTABLE USE POLICY

Boys & Girls Clubs of Silicon Valley is committed to providing a safe use of technology and online safety for members, staff and volunteers. The acceptable use policy provides the framework for those safety practices and procedures.

STAFF AND VOLUNTEER USAGE

Before a staff member or volunteer can use Club technology equipment or a personal device, he/she shall read and sign the Technology Acceptable Use policy and return it to the Club. Under the Technology Acceptable Use policy, the following relevant principles shall apply:

Club devices shall include any and all Club-owned existing and/or emerging technologies and devices that can take photographs, play and record audio or video, input text, upload and download content and/or media and transmit or receive messages or images.

Personally owned devices shall include any and all staff-owned existing and/or emerging technologies and devices that can take photographs, play and record audio or video, input text, upload and download content and/or media and transmit or receive messages or images. Personal devices are prohibited from being used during program hours unless directed by a supervisor.

Staff are prohibited from using cellphones during programmatic hours unless directed by a supervisor.

Club Purposes include but are not limited to the delivery of program activities, accessing sanctioned training or career development opportunities, communication with experts and/or authorized Club staff and for Club purposes or management of other Club activities, such as member check-in or incident reporting.

Staff are expected to act responsibly and thoughtfully when using technology resources. Staff bear the burden of responsibility to ask their supervisor when they are not sure of the permissibility of a particular use of technology prior to engaging in that use.

Authorized use: Personal devices are prohibited from being used during program hours unless directed by a supervisor.

The Club expressly prohibits the use of personally owned devices in locker rooms, restrooms and other areas where there is an expectation of privacy.

Appropriate use: Staff may not use any technology to harass, threaten, demean, humiliate, intimidate, or embarrass their peers or others in their community. Any inappropriate use of a personally owned device, as determined by a supervisor, can lead to disciplinary action including but not limited to confiscation of the device, immediate suspension from the Club, termination of employment or volunteer assignment or other disciplinary actions determined to be appropriate to the Club's existing disciplinary policies including, if applicable, referral to local law enforcement.

Monitoring and Inspection: Boys & Girls Clubs of Silicon Valley reserves the right to monitor, inspect, copy and review a personally owned device that is brought to the Club. Staff may refuse to allow such inspections. If so, the staff member may receive disciplinary action up to and including termination.

Loss and damage: Staff are responsible for keeping their assigned devices with them at all times. Supervisors and the Club at large are not responsible for the security and condition of the staff member's personal device. Furthermore, the Club is not liable for the loss, damage, misuse or theft of any personally owned device brought to the Club.

Any inappropriate or unauthorized use of a personally owned device, as determined by a supervisor, can lead to disciplinary action including but not limited to confiscation of the device, immediate suspension from the Club, termination of employment or volunteer assignment or other disciplinary actions determined to be appropriate to the Club's existing disciplinary policies, including, if applicable, referral to local law enforcement.

Inappropriate communication includes but is not limited to:

- Obscene, profane, lewd, vulgar, rude, inflammatory, threatening or sexual content or disrespectful language or images typed, posted or spoken by staff or members.
- Information that could cause conflict.
- Personal attacks, including prejudicial or discriminatory attacks.
- Harassment (persistently acting in a manner that distresses or annoys another person) or stalking others.
- Knowingly or recklessly posting false or defamatory information about a person or organization.

- Communication that promotes the destruction of property, including the acquisition or creation of weapons or other destructive devices.

If a staff member is told to stop sending communications, they must cease the activity immediately.

Staff must be aware of the appropriateness of communications when using Club or personally owned devices. Inappropriate communication is prohibited in any public or private messages, as well as material posted online.

Staff may not use any technology to harass, threaten, demean, humiliate, intimidate, embarrass or annoy others. This behavior is cyberbullying, which is defined as bullying that takes place using existing or emerging technologies and devices. Any cyberbullying that is determined to disrupt the safety and/or wellbeing of the Club, Club staff, Club members, volunteers, or community is subject to disciplinary action.

Examples of cyberbullying include but are not limited to:

- Harassing, threatening or hurtful text messages, emails or comments on social media.
- Rumors sent by email or posted on social networking sites.
- Use of embarrassing pictures, videos, websites or fake profiles.

Communication with Club members: Staff may never use personal devices to communicate directly with a single Club member. All communication between staff and Club members must include an additional staff member and at least two Club members. This also includes overnight events such as Keystone Conferences and Youth of the Year events.

Internet access: Personally owned devices used at the Club must access the internet via the Club's content-filtered wireless network and are not permitted to directly connect to the internet through a phone network or other content service provider. Boys & Girls Clubs of Silicon Valley reserves the right to monitor communication and internet traffic and to manage, open or close access to specific online websites, portals, networks or other services. Staff must follow Club procedures to access the Club's internet service.

CLUB MEMBER USAGE

Before a member will be allowed to use Club technology equipment or their personal device, both the member and their parent/guardian will need to read and sign the Technology Acceptable Use policy and return it to the Club. Under the Technology Acceptable Use policy, the following relevant principles shall apply:

Club devices shall include any and all Club-owned existing and/or emerging technologies and devices that can take photographs, play and record audio or video, input text, upload and download content and/or media and transmit or receive messages or images.

Personally owned devices shall include any and all member-owned existing and/or emerging technologies and devices that can take photographs, play and record audio or video, input text, upload and download content and/or media and transmit or receive messages or images.

Club purposes shall include program activities, career development, communication with experts and/or Club peer members, homework and Club activities. Members are expected to act responsibly and thoughtfully when using technology resources. Members bear the burden of responsibility to inquire with staff when they are unsure of the permissibility of a particular use of technology prior to engaging in its use.

Authorized use: Club devices and personally owned devices are permitted for use during approved Club times for Club purposes and in approved locations only. The Club expressly prohibits the use of Club devices or personally owned devices in locker rooms, restrooms and other areas where there is an expectation of privacy.

Appropriate use: Members may not use any technology to harass, threaten, demean, humiliate, intimidate, embarrass or annoy their peers or others in their community. Any inappropriate use of a Club or personally owned device, as determined by Club staff, can lead to disciplinary action including but not limited to confiscation of the device, immediate suspension from the Club, termination of membership or other disciplinary actions determined to be appropriate to the Club's existing disciplinary policies including; if applicable, referral to local law enforcement.

Monitoring and Inspection: Boys & Girls Clubs of Silicon Valley reserves the right to monitor, inspect, copy and review any personally owned device that is brought to the Club Parents/guardians will be notified before such an inspection takes place and may be present, at their choice, during the inspection. Parents/guardians may refuse to allow such inspections. If so, the member may be barred from bringing personally owned devices to the Club in the future.

Loss and damage: Members are responsible for keeping devices with them at all times. Staff are not responsible for the security and condition of the member's personal device. Furthermore, the Club is not liable for the loss, damage, misuse or theft of any personally owned device brought to the Club.

Any inappropriate or unauthorized use of a Club or personally owned device, as determined by Club staff, can lead to disciplinary action including but not limited to confiscation of the device,

immediate suspension from the Club, termination of membership or other disciplinary actions determined to be appropriate to the Club's existing disciplinary policies, including, if applicable, referral to local law enforcement.

Members must be aware of the appropriateness of communications when using Club or personally owned devices. Inappropriate communication is prohibited at all times, as well as material posted online. Inappropriate communication includes but is not limited to the following:

- Obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language or images typed, posted or spoken by members;
- Information that could cause damage to an individual or the Club community or create the danger of disruption of the Club environment;
- Personal attacks, including prejudicial or discriminatory attacks;
- Harassment (persistently acting in a manner that distresses or annoys another person) or stalking of others;
- Knowingly or recklessly posting false or defamatory information about a person or organization; or
- Communication that promotes the destruction of property, including the acquisition or creation of weapons or other destructive devices.

If a member is told to stop sending communications, that member must cease the activity immediately.

Cyberbullying

Members may not utilize any technology to harass, threaten, demean, humiliate, intimidate, embarrass or annoy their peers or others in their community. This behavior is cyberbullying, which is defined as bullying that takes place using emerging technologies and devices. Any cyberbullying that is determined to disrupt the safety and/or well-being of the Club, Club members, Club staff or community is subject to disciplinary action.

Examples of cyberbullying include, but are not limited to:

- Harassing, threatening or hurtful text messages, emails or comments on social media.
- Rumors sent by email or posted on social networking sites.
- Embarrassing pictures, videos, websites or fake profiles.
- Members may not attempt to gain unauthorized access to the Club's network, or to any other computer system through the Club's network.
    - This includes attempting to log in through another person's account or accessing another person's files.

- Members may not use the Club's network to engage in any illegal act, including, but not limited to, arranging for the purchase or sale of alcohol, tobacco or other drugs; engaging in criminal activity; or threatening the safety of another person.
- Members may not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses.

Internet access: Personally owned devices used at the Club must access the internet via the Club's content-filtered wireless network and are not permitted to directly connect to the internet through a phone network or other content service provider. Boys & Girls Clubs of Silicon Valley reserves the right to monitor communication and internet traffic, and to manage, open or close access to specific online websites, portals, networks or other services. Members must follow Club procedures to access the Club's internet service.

Parental notification and responsibility: While Boys & Girls Clubs of Silicon Valley's Technology Acceptable Use Policy restricts the access of inappropriate material; supervision of internet usage might not always be possible. Due to the wide range of material available on the internet, some material might not fit the particular values of members and/or their families. Because of this, it is not considered practical for Boys & Girls Clubs of Silicon Valley to monitor and enforce a wide range of social values in student use of the internet. If parents/guardians do not want members to access information beyond the scope of the Technology Acceptable Use Policy, they should instruct members not to bring their device.

Digital citizenship: Club members shall conduct themselves online in a manner that is aligned with Boys & Girls Clubs of Silicon Valley Code of Conduct. The same rules and guidelines members are expected to follow offline (i.e., in the real world) shall also be followed when online. Should a member behave online in a manner that violates Boys & Girls Clubs of Silicon Valley's Code of Conduct, that member shall face the same discipline policy and actions they would if their behavior had happened within the physical Club environment.

Club-owned-and-operated technology: Members are expected to follow the same rules and guidelines when using Club-owned technology. Club technology and systems are the property of the Club, are intended to be used for Club purposes and are to be used during approved times with appropriate supervision. Club members shall never access or use Club technology or systems without prior approval.

Digital citizenship and Technology Safety training: All members who wish to use a Boys & Girls Clubs device or equipment will be required to successfully complete a BGCA-provided digital citizenship and technology safety training. This training is required for all members annually.

SOCIAL MEDIA USE POLICY

Social network sites can be defined as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site. Examples include but are NOT limited to, Facebook, Instagram, LinkedIn, Twitter, etc. This policy separates the issue of participation into "personal" and "work-related" activities.

- Employees and volunteers are prohibited from using personal social media sites, blogs, Facebook, Instagram and other such sites to communicate with club members. Club persons and volunteers who maintain personal web pages, blogs, or social networking sites such as Facebook, Instagram, and Twitter are encouraged to make these Internet sites “private” rather than granting general access to all users.
- It is inappropriate for employees to communicate with Club members using personal social media, regardless of the reason.
    - Employees shall not “friend” or connect with club members on personal social media sites. Information published on personal blogs or social media sites should comply with Club confidentiality and disclosure policies.
    - Club employees are asked to be respectful of our organization, other employees, volunteers, and our members when communicating with the public using the Internet.
    - Employees are prohibited from taking or posting personal photos of program activities to their social media sites.
- Staff may not use social media to violate any Club policies. Each situation by which an employee’s use of social media may violate Club policy cannot be detailed. Below are basic principles that govern the use of social media by Club employees. An employee who has a question about whether their use of social media is prohibited by this policy should contact their manager or Human Resources before engaging.
- While the use of these sites is becoming commonplace, it is important that staff personnel remember to conduct themselves in an appropriate manner. The goal is to help employees avoid any unintended situations that could adversely affect their professional standing with the Club. These guidelines are not intended to restrict participation by employees or violate the employee’s right to communicate, but rather to provide some level of protection if they choose to engage in online activities.

APPROPRIATE USE OF SOCIAL MEDIA:

- Personal blogs/posts should have clear disclaimers that the views expressed by the author are the author's alone and do not represent the views of the Club.
    - Make your writing clear that you are speaking for yourself and not on behalf of Boys & Girls Clubs of Silicon Valley either officially or unofficially.
- Information published on your blogs/posts should comply with Club confidentiality and disclosure of proprietary information & conflict of interest policies. This also applies to comments posted on other blogs, forums, and social networking sites.
- Be respectful to Boys & Girls Clubs policies, other employees, volunteers, Club members and their families.
- Be thoughtful when posting items online (e.g., photographs) as some may be considered offensive to other parties and a violation of other Club policies.
- Social media activities should not interfere with work commitments.
    - Employees are prohibited from engaging in social media during their working time regardless of whose equipment and technology are used.
    - Any posts made to your account using Club equipment might be stored on Club servers and may be accessed at any time.
- Your online presence reflects the Club. Be aware that your actions captured via images, posts, or comments can reflect on the Club.
- Never post information that is considered proprietary, copyrighted, defamatory, libelous, or obscene (as defined by the courts) or harassing in any way.
- Respect our audience. Do not use ethnic slurs, personal insults, obscenity, or engage in any conduct that would not be acceptable in the Club or violate any of Club policies.
- Use your best judgment. Remember that there are always consequences to what you publish. If you are about to publish something that makes you even the slightest bit uncomfortable, review the rules above and think about why. If you are still unsure, and it is related to the Club, feel free to discuss it with your manager or Human Resources. However, you have sole responsibility for what you post to your blog or publish in any form of online social media.
- You also have responsibility over what others post and publish on your social media/networking site. The above rules apply to comments and blogs posted by others on your site. Please exercise your best professional judgment and take the most prudent action possible when posting and monitoring your web-based social media/networking sites.
- Employees and volunteers must comply with the Terms of Service of each site you use. Boys & Girls Clubs of Silicon Valley does not maintain any legal responsibility for employee's use of social media. Employees and volunteers are legally responsible for their own use of social media.

- The Club reserves the right to monitor employee use of social media.
- Any violations of this or any Club policies may lead to disciplinary action up to and including termination of employment.

TRANSPORTATION POLICY

Boys & Girls Clubs of Silicon Valley is committed to providing a safe environment and enforces the following transportation policy for members, staff, volunteers and other adults. Boys & Girls Clubs of Silicon Valley only provides transportation to and from the Clubhouse and various approved off-site locations. The Club only transports youth in Club vehicles or other vehicles approved by Club leadership.

DRIVERS

- Must allow for DMV background check and be cleared to transport youth per the barrier crime policy of the organization.
- Must be on the approved BGCSV Driver's List to drive Club members.
- Must be 21 years of age or older with a valid California's Driver's License.
- Proof of personal insurance.
- Must have completed all of in person and/or online BGCSV driver training courses.
- Must keep an updated list of all youth who are transported to and from the Clubhouse and Club related activities.
- Must confirm that no children are left on a vehicle after every trip (based on a seat-by-seat scan of each vehicle); log must be signed daily to ensure compliance
- Must perform regular checks to ensure that all members are picked up and dropped off at the appropriate times and locations.
- Must submit written reports detailing issues or incidents involving transportation of members to and from the Clubhouse or to and from Club-related activities.
- Must only transport members in official Club vehicles.
- Must ensure that at least three individuals are present when transporting members. If one child remains to be dropped off, two adults (18 or over) must be present in the vehicle.
- Must never transport Club members in personal vehicles.
- Must never use cell phones, PDAs or other communication devices while transporting members to and from the Clubhouse or Club-related activities.

VEHICLE

- GPS devices are installed on all BGCSV vehicles and driving speeds will be recorded and monitored.
- Each vehicle should meet all local, state and federal inspection and licensing requirements.
- Each vehicle should be inspected as outlined by DMV by staff before every trip for which youth are being transported; any problems with the vehicle must be addressed promptly.
- Regular maintenance should be performed on vehicles and documents/records reflecting that maintenance should be maintained.
- Each vehicle must provide a seat belt for every passenger and fully comply with state and federal seat belt regulations.
- Each vehicle must have a complete first-aid kit that satisfies state licensing requirements
- Each vehicle must have a working and current fire extinguisher that satisfies state licensing requirements.
- Each vehicle must have reflective traffic warning signs (e.g., triangles or flares) that are stored securely during transport.
- The vehicle must be clean and well maintained and exterior physical damage must be repaired promptly.

ACCIDENT OR EMERGENCY PROTOCOL

- Drivers should immediately notify Club leadership if there is a delay or issue (e.g., breakdown, accident, emergency) with transporting members to and from the Clubhouse or Club-related activities.
- Staff shall immediately inform Club leadership if a staff member, volunteer or board member violates this policy. In such cases, the organization will take appropriate disciplinary action, up to and including termination.

EMERGENCY OPERATIONS PLAN POLICY (in process)

Through the appropriate use of Club and community resources, Boys & Girls Clubs strive to mitigate the immediate effects of an emergency and its long-term effects on Club operations and mission by being prepared to effectively respond to and recover from an emergency.

EMERGENCY OPERATIONS PLAN (EOP)

Boys & Girls Clubs shall create and maintain an Emergency Operations Plan (EOP). At minimum, the plan shall encompass the following elements:

- Mitigation, preparedness, response and recovery for the following emergencies:
  - Earthquake
  - Fire
  - Weather (flooding,hurricane,etc.)
  - Lockdown (for interior or exterior threat)
  - Bomb Threat
  - Suspicious Package

Training/drill schedule and reporting procedures for staff, volunteers and members. Developed and shared with local first responders, such as fire departments and law enforcement agencies.

EOP ANNUAL REVIEW

Boys & Girls Clubs of Silicon Valley leadership will maintain a board-led safety committee that regularly focuses on safety and will have oversight and responsibility for the emergency operations plan. The board-led safety committee will be responsible for reviewing and updating the emergency operations plan annually.

FIRST AID AND CPR TRAINING

Boys & Girls Clubs of Silicon Valley always maintains a minimum of one CPR or first-aid-trained staff on site during all operating hours when members are being served. Boys & Girls Clubs of Silicon Valley will provide annual training to ensure that all staff have a valid CPR or first-aid-training certificate.

EMERGENCY SUPPLY TUB

Boys & Girls Clubs of Silicon Valley always maintains an Emergency Preparedness Tub at each of its Club sites. Each tub contains the supplies needed to maximize survival during any emergency event.

- Flashlights (3)
- Batteries ('D' cell)
- Water (15 gallons)
- Portable radio
- First aid kit
- Matches
- Tool kit
- Paper products (e.g., toilet paper, paper towels).
- Food supplies
- Emergency supplies are kept in a red plastic tub (red to designate emergency)
- AEDs

EMERGENCY CONTACTS

Please use the below contacts in case of emergencies:

- Ambulance: 9-1-1
- Fire: 9-1-1
- San Jose Police Department: (408) 277-8900
- Morgan Hill Police Department: (408) 779-2101
- Redwood City Police Department: (650) 780-7100
- Concord Police Department: (925) 671-3220
- Antioch Police Department: (925) 779-6900

In any emergency, make sure to notify your immediate Supervisor about the emergency.

KEY DEFINITIONS

Emergency: An emergency is any event, natural or man-made, that places life or significant Club assets in danger or threatens the ability to conduct normal business operations and usually involves abnormal time constraints and responses.

Mitigation: Mitigation is the effort to reduce loss of life and property by lessening the impact of disasters or emergencies. For mitigation to be effective, we need to take action now — before the next emergency occurs — to reduce human and financial consequences later.

Preparedness: Preparedness helps everyone act quickly and decisively in the face of a disaster or emergency and can minimize loss of property and prevent death and injury. An effective emergency plan should include steps to ensure that those with disabilities or special needs are provided with a proper evacuation strategy.

RESOURCES

LINK TO Crisis Management Plan

LINK TO Emergency Operations Plan

Safety Committee Members:

Name	Title	Phone	Contact Email
Steve Wymer	CEO	408-404-4890	steve.wymer@bgclub.org
Mark Washbush	COO	408-889-1362	mark.washbush@bgclub.org
Kelli O'Gorman	CFO	408-914-2243	kelli.ogorman@bgclub.org
Helen Sustarich	Safety & Compliance Coordinator	408-457-8354	helen.sustarich@bgclub.org
Angela Roach	Board Member		angela.roach@analog.com
Sean Heywood	Board Member		sean.a.heywood@gmail.com

BOYS & GIRLS CLUBS
OF SILICON VALLEY

The BGCSV Safety Acknowledgment

I have read and understand Boys & Girls Club of Silicon Valley's Safety Handbook and its requirements and expectations of me as an employee.

I _____, acknowledge that I have received a copy of the Safety Handbook and will abide by the procedures and policies as stated in such:

Signature: _____ Date: _____