TECHNOLOGY ACCEPTABLE USE

for Members, Employees & Volunteers

BOYS & GIRLS CLUBS
OF THE CHATTAHOOCHEE VALLEY

Revised July 2025

1. Summary of the Technology Acceptable Use Policy

1. This Policy applies to employees, volunteers and Club members. Please review the entire policy for complete information. Before an **employee or volunteer** can use Club technology equipment or a personal device, he/she shall read and sign this Technology Acceptable Use policy and return it to the Club. Before a **member** is allowed to use Club technology equipment or their personal device, both the member and his/her parent/guardian will need to read and sign the Technology Acceptable Use policy and return it to the Club.

2. Club devices and personally owned devices are permitted for use during approved Club times for Club purposes and in approved locations only.

3. You may not use Club devices or personally owned devices in locker rooms, restrooms and other areas where there is an expectation of privacy.

4. Do not use technology to harass, threaten, demean, humiliate, intimidate, embarrass or annoy another person.

5. We reserve the right to monitor, inspect, copy and review files stored and emails or other messages received and sent on Club-owned devices or networks. We also reserve the right to inspect and/or review personally owned devices that are brought to the Club.

6. Do not send inappropriate, obscene, rude, threatening, defamatory, disrespectful or other information that could cause conflict or damage to another person.

7. Staff may not use a personal device to communicate directly with a single Club member.

8. Do not try to gain unauthorized access to the Club's network or any computer system.

9. Do not use technology for illegal acts.

10. Employees may only use cell phones for Club purposes while supervising Club members.

11. All Club members must follow the Club's Code of Conduct during both offline and online activities.

12. Club members must complete BGCA-provided digital citizenship and technology safety training before they can use technology inside a Club.

2. Technology Definitions & Responsibility

Based on the model BGCA Technology Acceptable Use Policy

BGCCV is committed to providing a safe use of technology and online safety for members, staff and volunteers. This acceptable use policy provides the framework for those safety practices and procedures.

Before an **employee or volunteer** can use Club technology equipment or a personal device, he/she shall read and sign this Technology Acceptable Use policy and return it to the Club. Before a **member** will be allowed to use Club technology equipment or their personal device, both the member and

his/her 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 individually-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 for **employees and volunteers** 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 aren't sure of the permissibility of a particular use of technology prior to engaging in that use.

Club purposes **for members** 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.

3. Authorized Use of Technology

Based on the model BGCA Technology Acceptable Use Policy

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.

Only software that is authorized by BGCCV may be used, copied or installed on Club devices.

4. Appropriate Use of Technology

Based on the model BGCA Technology Acceptable Use Policy

By Employees & Volunteers: Employees and volunteers may not use any technology to harass, threaten, demean, humiliate, intimidate, embarrass or annoy their peers or others in their community. Any inappropriate or unauthorized use of a Club or 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.

By Members: Members may not use any technology to harass, threaten, demean, humiliate, intimidate, embarrass or annoy their peers or others in their community. 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.

5. Monitoring and Inspection

Based on the model BGCA Technology Acceptable Use Policy

Boys & Girls Clubs of the Chattahoochee Valley reserves the right to monitor, inspect, copy and review files stored and emails or other messages received and sent on Club-owned devices or networks. In addition, BGCCV reserves the right to inspect and/or review personally owned devices that are brought to the Club.

For Employees: Staff may refuse to allow such inspections. If so, the staff member may disciplinary action up to and including termination

For Members: 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.

6. Loss and Damage

Based on the model BGCA Technology Acceptable Use Policy

Members, employees and volunteers are responsible for keeping devices with them at all times. Furthermore, members, employees and volunteers will be liable for any loss or damage they cause to Club-owned devices.

Staff, supervisors and the Club at large are not responsible for the security and condition of an individual's personal device. The Club is not liable for the loss, damage, misuse or theft of any personally owned device brought to the Club.

7. Communicating with Technology

Based on the model BGCA Technology Acceptable Use Policy

All messages composed, sent or received on Club devices are and remain the property of BGCCV. They are not the private property of any employee.

Members, employees and volunteers 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.

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, volunteers or members.
- Information that could cause conflict.
- 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 others.
- Knowingly or recklessly posting false or defamatory information about a person or organization.
- Copyrighted materials, trade secrets, confidential and proprietary information
- Communication that promotes the destruction of property, including the acquisition or creation of weapons or other destructive devices.

If a Club member, employee or volunteer is told to stop sending communications by a supervisor, he/she must cease the activity immediately.

8. Cyberbullying

Based on the model BGCA Technology Acceptable Use Policy

Members, employees and volunteers 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 well-being of the Club, Club staff, Club members 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.

9. Communicating with Club Members

Based on the model BGCA Technology Acceptable Use Policy

Staff may never use personal devices to communicate directly with a single Club member. Proper protocol dictates that 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.

10. Internet Access

Based on the model BGCA Technology Acceptable Use Policy

The Internet can provide our members with exciting and enriching opportunities for educational, cultural and recreational experiences. Offering our member's exposure to the Internet and teaching them safe and responsible ways of using it are important components of BGCCV's technology mission to prepare our youth for competency in an information-driven, global society. However, in an unsupervised and irresponsible environment, the Internet can expose our members to unsafe situations.

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. BGCCV 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. BGCCV reserves the right to install blocking and other software on Club devices to prevent access to certain sites on the internet. Members, employees and volunteers must follow Club procedures to access the Club's internet service.

11. Passwords and Access

Based on the model BGCA Technology Acceptable Use Policy

To prevent unauthorized access, devices must lock themselves and require authentication using the strongest features available on the device. A minimum standard would require a typed password of at least six characters or numbers, though some devices utilize fingerprint or other biometric technologies.

Employees and volunteers are prohibited from sharing their user ID and password. Employees and volunteers are also prohibited from using another person's user ID and/or password.

Employees and volunteers must share their user ID and/or password with BGCCV for any software or technology they utilize to perform their duties.

12. Unauthorized Access

Based on the model BGCA Technology Acceptable Use Policy

Members, employees and volunteers 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, staff, guest and volunteers 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, staff, guests and volunteers may not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses.

Only software that is authorized by BGCCV may be used, copied or installed on Club devices.

13. Cell Phone Usage by Employees

Based on the model BGCA Technology Acceptable Use Policy

Employees may never use electronic devices such as cell phones, PDAs or other communication devices while supervising members unless for Club purposes. If an employees needs to make or take a call for an emergency, please notify your supervisor and ask that another employee supervise your group/area while you are on the phone.

Texting while supervising youth is not permitted. Texting while working, when not directly supervising youth, should be work related. Occasional personal texts are permitted. However, if you are texting or conducting other personal business while working, your supervisor can issue disciplinary notification.

14. Employee Social Media Use

BGCCV recognizes that employees may engage with social media platforms while off duty. "Social networking" for purposes of this policy includes all types of postings on the Internet, including postings on social networking sites (such as Facebook©, Snapchat©, TikTok© Instagram© or LinkedIn©, etc.), blogs and other on-line journals and diaries, bulletin boards and chat rooms, "microblogging," such as X/Twitter©; and the posting of videos on YouTube© and similar media. Social networking also includes permitting or not removing postings by others where an employee can control the content of postings, such as on a personal profile or blog. This policy applies regardless of whether the employees is social networking while on or off duty.

Employees who engage in social networking should be mindful that their postings, even if done off premises and while off duty, could affect, either positively or negatively, BGCCV'S interests or reputation. In addition, some readers may view you as a spokesperson for BGCCV. To reduce the likelihood that your personal social networking will harm BGCCV, we ask that you observe the following guidelines when social networking.

- Do not engage in social networking using any of BGCCV'S electronic resources, such as your work computer.
- Your social networking is subject to all of the policies of the organization, as well as BGCCV'S Employee Handbook. You are specifically prohibited from disclosing any information about BGCCV'S members, including the fact that a particular individual is a member at BGCCV.
- BGCCV has spent substantial time and resources building its reputation and good will which are valuable and important assets. Before you engage in any social networking that identifies yourself as an employee of BGCCV or that identifies BGCCV, please consider whether you are damaging BGCCV'S reputation.
- You are more likely to resolve complaints about work by speaking directly with your co-workers, supervisor or other management-level personnel than by posting complaints on the Internet. Nonetheless, if you decide to post complaints or criticism, avoid doing so in a way that is defamatory or damaging to BGCCV and any of BGCCV'S employees or be prepared to face possible legal consequences.
- BGCCV will review your social networking activities at its discretion. Please note that this policy applies even if your social networking is anonymous or under another name. If you engage in such social networking, you should be aware that in appropriate circumstances BGCCV will take steps to determine your identity.
- Failure to comply with this policy may lead to discipline, up to and including termination of employment. BGCCV will pursue all available legal remedies. BGCCV also may report suspected unlawful conduct to appropriate law enforcement authorities.

15. Generative Artificial Intelligence Use

Based on the model BGCA Generative Artificial Intelligence Policy

Boys & Girls Clubs of the Chattahoochee Valley continues to support innovation through technology and recognizes the potential benefits of artificial intelligence (AI), specifically generative AI, in enhancing our products, services, and operations. While we remain committed to adopting new technologies to aid the organization, we must seek to understand and acknowledge the potential risks and ethical concerns associated with AI, including issues related to bias, privacy, security, and transparency. As such, we are committed to ensuring the responsible and ethical use of AI in our organization.

Employees wishing to use generative AI can utilize the free platforms available; however, if the job duties require a purchased license this requires approval from the Administrative Office.

All AI-generated content must be reviewed for accuracy and significance before relying on it for work purposes. If a reliable source cannot be found to verify factual information generated by the AI solution, that information cannot be used for work purposes.

Acceptable uses for AI-generated content include:

- For general-knowledge questions meant to enhance an employee's understanding on a work related topic.

- To brainstorm ideas related to projects you are working on.
- To create formulas for Excel spreadsheets or similar programs.
- To develop or debug code, to be verified before deployment.
- To draft an email or letter.
- To summarize online research or to create outlines for content projects to assist in full coverage of a topic.

Avoid entering sensitive or identifying data into these platforms, this includes, but is not limited to entering personally identifiable information, business credentials, financial information, or phone numbers into the generative prompts. Further, business sensitive or proprietary data (that is, information if it became public would put at risk our organization's reputation, proprietary information, and any personal or financial information of staff, volunteers or youth) must not be entered in generative AI solutions or solutions that have generative AI features.

16. Technology-Specific Rules for Club Members & Parents

Parental notification and responsibility: While the Boys & Girls Clubs of the Chattahoochee Valley 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 BGCCV 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 access such materials.

Digital citizenship: Club members shall conduct themselves online in a manner that is aligned with the Boys & Girls Clubs of the Chattahoochee 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 the BGCCV 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.

17. Acknowledgment

I am aware of the Technology Acceptable Use Policy and agree to abide by the policy:

Member Signature (if applicable)	Date:
Member Name (if applicable)	
Parent / Guardian Signature (if applicable)	Date:
Parent / Guardian Name (if applicable)	
Employee / Volunteer Signature (if applicable)	Date:
Employee / Volunteer Name (if applicable)	