



Technology Acceptable Use Policy

Authorization Date: November 14, 2023

Policy Statement

Boys & Girls Clubs of Greater Kalamazoo 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 and was adapted from the Boys & Girls Clubs of America policy. Under the Technology Acceptable Use policy, the following relevant principles shall apply:

MEMBER USAGE

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.

GREAT FUTURES START **HERE.**



Members 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 recorded or 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.

Monitoring and inspection: Boys & Girls Clubs reserves the right to monitor, inspect, copy, and review any personally owned device that is brought to the Club and Club-owned devices or networks including files stored. 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 personal 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.

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.

GREAT FUTURES START **HERE.**



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 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 the 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 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 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 Boys & Girls Clubs 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

GREAT FUTURES START **HERE.**



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.

STAFF AND VOLUNTEER USAGE

In addition to abiding by and being held accountable to the same principles as outlined above under Member Usage, staff and volunteers must also follow these additional principles:

Communication with Club members: Staff should never use personal devices to communicate directly with a single Club member. If there is no other option than to use a personal device, a privacy app like GroupMe or Google Voice must be used. Proper protocol dictates that all communication between staff and Club members must include at least one additional staff member and only if necessary for approved targeted programs. This also includes overnight events such as Keystone Conferences and Youth of the Year events. Explicit and written permission must be obtained from the Chief Executive Officer for any exceptions. This policy works in conjunction with the BGCA requirements for employing youth workers.

Privacy Rights in the Workplace: Employees are restricted from video and audio recording coworkers at work especially in secret or to capture conflict or to provide “evidence” of misconduct or other behavior that may result in disciplinary action.

Monitoring and inspection: Boys & Girls Clubs 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 be subject to disciplinary action up to and including termination.

Password and access: 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.