

**GREAT FUTURES START HERE.**



**BOYS & GIRLS CLUB  
OF WESTERN LANE COUNTY**

**CHILD SAFETY**

**ACCEPTABLE TECHNOLOGY USE POLICY**

<b>CATEGORY:</b> Child Safety	<b>APPROVED:</b> November 22, 2022
<b>APPROVING AUTHORITY:</b> BGCWLC Board of Directors	<b>LAST UPDATE:</b> October 31, 2022
<b>CONTACT:</b> BGCWLC CEO	<b>NEXT REVIEW:</b> October 31, 2023

## Acceptable Technology Use Policy

The Boys & Girls Clubs of Western Lane County (Club) is committed to providing a safe use of technology and online safety for Club members, staff, volunteers, and board members. The acceptable use policy provides the framework for those safety practices and procedures.

### **Club Member Usage**

Before Club members are allowed to use Club devices or their personal device, both the member and their parent/guardian will need to read and sign the Acceptable Technology Use policy and return it to the Club. Under the Acceptable Technology 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.

**Personal 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.

- Acceptable Personal Devices
  - Cell phones-Teen Center only (for parent/family communication)
  - School provided laptops or tablets- For schoolwork only
  - Smartwatches- Teen Center only (for parent/family communication)
- Unacceptable Personal Devices
  - All emerging technologies or 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.
  - Cameras
  - Cell phone-Elementary
  - Gaming devices
  - Smartwatches-Elementary

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

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

**Appropriate Use:** Club 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 personal device 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.

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

**Cyberbullying:** Club 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.
- Use of embarrassing pictures, videos, websites, or fake profiles.

**Monitoring and Inspection:** The Club reserves the right to monitor, inspect, copy, and review any personal device in the event of suspected inappropriate use. 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 personal devices to the Club in the future.

**Loss or Damage:** Club members are responsible for securing devices 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 personal device brought to the Club.

**Internet Access:** Acceptable personal 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. The Club 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. Club members must follow Club procedures to access the Club's internet service.

**Parental Notification and Responsibility:** While this 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 their families. Because of this, it is not considered practical for the Club to monitor and enforce all internet activity. If parents/guardians do not want members to access information beyond the scope of this policy, they should instruct members not to access such materials.

### **Staff, Volunteer, and Board Member Usage**

Before staff, volunteers, or board members are allowed to use Club devices or their personal device, they will need to read and sign the Acceptable Technology Use policy and return it to the Site Director, CEO, or Board President. Under the Acceptable Technology Use policy, the above principles (club devices, personal devices, club purposes, authorized use, appropriate use, cyberbullying, monitoring and inspection, and loss or damage) stated under the Club Member Usage section apply to staff, volunteers, and board members as well as the following principles.

Any inappropriate or unauthorized use of a personal device can lead to disciplinary action including but not limited to 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.

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

**Communication with Club members:** Staff, volunteers, and board members may never use personal devices to communicate directly with a single Club member. All communication with Club members must include an additional staff, volunteer, or board member and at least two Club members.

**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.