WAKEMAN
BOYS & GIRLS CLUB

Technology Acceptable Use Policy

Wakeman Boys & Girls Club's (WBGC) computer network and internet access are available to members to enhance their educational experience and help them become literate in a technological world.

The purpose of this Acceptable Use Policy is to foster the appropriate use of that network, email, social media and the internet and maintain a safe and secure environment for members, staff, volunteers, and others. The following guidelines apply to all users, whenever they access any of the WBGC's network connections or use any device for club purposes.

PART I: CLUB MEMBER USAGE

Under the Technology Acceptable Use Policy, the following principles shall apply:

Club devices shall include any and all WBGC-owned or controlled 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 or controlled existing and/or emerging technologies and devices, including school-provided 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. Emerging technologies and devices include but are not limited to cell phones, computers, tablets, and storage media (e.g., flash drives), as well as communication tools including social media sites, text messages, chat, and websites. Unacceptable devices in this policy include but are not limited to, gaming devices or consoles, laser pointers, modems or routers, and televisions unless specifically authorized by the Unit Executive Director.

Club purposes shall include program activities, career development, communication with experts and/or Club peer members, homework, and WBGC 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.

Inappropriate Communications. Members must be aware of the appropriateness of communications when using club devices, 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 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 WBGC community or create the danger of disruption of the WBGC 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 WBGC, Club members, Club staff or community is subject to disciplinary action.

Examples of cyberbullying include, but are not limited to:

- Harassing, mean, 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 must not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses. Members must not use the WBGC'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.

Plagiarism and copyright infringement. Members must not plagiarize works found on the internet. Plagiarism is taking ideas, writing or pictures of others and presenting them as your own. It is dishonorable, and it is a prohibited use of the WBGC's facilities.

Members must respect the rights of copyright owners. Copyright infringement occurs when you reproduce a work that is protected by a copyright without authorization. If a work contains language that specifies appropriate use of that work, the expressed requirements must be followed. Copyright law can be confusing; therefore, if you have any questions, please ask WBGC staff.

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

Consequences for inappropriate use: Any inappropriate use of a WBGC or personally owned device, as determined by WBGC staff, can lead to disciplinary action including but not limited to confiscation of the device, immediate suspension from the WBGC, termination of membership or other disciplinary actions determined to be appropriate to the WBGC's existing disciplinary policies including, if applicable, referral to local law enforcement.

Unauthorized access: Members may not attempt to gain unauthorized access to WBGC's network, or to any other computer system through the WBGC's network. This includes attempting to log in through another person's account or accessing another person's files. Members may not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses.

Network Safety: WBGC's network has been established for educational purposes limited to classroom activities, school-to-career development, and scholastic research on appropriate subjects. WBGC's network has not been established as a public access service or a public forum. WBGC has the right to place reasonable restrictions on the material member's access or post through the system.

WBGC's network is considered a limited forum, similar to a school, and, therefore, WBGC reserves the right to regulate that forum for valid educational reasons. WBGC will not restrict speech on the basis of a disagreement with opinions you, the members, are expressing. You should expect only limited privacy with the content of your personal files on WBGC's network. This situation is similar to the rights a student would have in the privacy of their locker at school. WBGC reserves the right to search files, if there is a reasonable suspicion someone violated this Acceptable Use Policy, Club rules and policies, or the law.

Parental notification and responsibility: While the WBGC'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 WBGC 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 WBGC 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 WBGC'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 WBGC-owned technology. WBGC technology and systems are the property of WBGC, are intended to be used for WBGC purposes, and are to be used during approved times with appropriate supervision. Club members shall never access or use WBGC technology or systems without prior approval.

PART II: STAFF AND VOLUNTEER USAGE

Under the Technology Acceptable Use Policy, the following relevant principles shall apply to staff and volunteers:

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.

Club Purposes: Shall include but are not limited to the delivery of program activities, accessing sanctioned training or career development opportunities, communication with experts and/or authorized WBGC staff and for WBGC purposes or management of other WBGC 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: Personally owned devices are permitted for use during approved WBGC times for WBGC purposes and in approved locations only. WBGC 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 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.

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 WBGC, termination of employment or volunteer assignment or other disciplinary actions determined to be appropriate to WBGC's existing disciplinary policies including, if applicable, referral to local law enforcement.

Monitoring and inspection: WBGC reserves the right to monitor, inspect, copy, and review a personally owned device that is brought to WBGC. Staff may refuse to allow such inspections. If so, the staff member may face disciplinary action up to and including termination.

Staff and volunteers must be aware of the appropriateness of communications when using club devices, 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 the following:

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.
- 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 of weapons or other destructive devices.
- Note that it is the responsibility of all staff and volunteers to convey the values of the Club to all its members. Staff and volunteers should avoid all public communications that are in conflict with those values as expressed in this policy.

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

Staff 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.

Communication with Club members: Staff and volunteers 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. This prohibition does not apply where the staff or volunteer and the member are related, or where there is a prior existing relationship that has been disclosed in advance to, and acknowledged by, the unit director.

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.

Disallowed apps and/or websites: WBGC expects that staff and volunteers will only access work-related content. WBGC does not allow staff to access sites that may include, but are not limited to: Gaming, gambling, adult content, illegal activities, or others that the organization deems inappropriate.

Part III: Generally Applicable Provisions

Under the Technology Acceptable Use Policy, the following relevant principles shall apply to members, staff and volunteers:

Monitoring and inspection: WBGC reserves the right to monitor, inspect, copy, and review a personally owned device that is brought to WBGC. Staff may refuse to allow such inspections. If so, the staff member may be subject to disciplinary action up to and including termination.

Internet access: Personally owned devices used at WBGC must access the internet via WBGC's content-filtered wireless network and are not permitted to directly connect to the internet through a phone network or other content service provider. WBGC 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 WBGC's procedures to access the WBGC's internet service.
Loss and damage: Members, staff and volunteers are responsible for keeping devices with them at all times. Supervisors and WBGC at large are not responsible for the security and condition of any personal device.

Furthermore, WBGC is not liable for the loss, damage, misuse, or theft of any personally owned device brought to WBGC.