BGCNAL Acceptable Computer Usage Policy

I. Overview

This policy covers the computer and Internet usage that is acceptable when utilizing Boys & Girls Clubs of North Alabama (BGCNAL) information systems.

II. Purpose

Boys & Girls Clubs of North Alabama's information systems are for legitimate business purposes only. Any unacceptable use or illegal activity can endanger the security and privacy of sensitive information and other business systems and create unnecessary business risks.

III. Scope

All users of any Boys & Girls Clubs of North Alabama-owned/controlled computer and network systems—including access to BGCA-hosted Websites and Applications

A. Exceptions

Any exceptions to the policies set forth in this document will require the approval of HR, General Counsel, and IT senior management.

B. Policy statement

Boys & Girls Clubs of North Alabama computers and networks are intended for business purposes only. All use is subject to monitoring. There is no right to privacy when using company equipment. The following specific requirements are in effect:

C. General Usage

- Users must not knowingly violate any local, state, federal, or international laws while using company information systems
- Users must not change the computer date or time or disable any anti-virus, personal firewall, or other security software at any time without the approval of the information security officer

D. Security Incident Reporting

All users must report any confirmed or suspected security incidents such as malware outbreaks, suspicious activity, hacker threats, or social engineering attempts to the information security officer immediately.

E. Passwords

Passwords are an important aspect of information security. A poorly chosen password may result in unauthorized access and/or exploitation of Boys and Girls Clubs of North Alabama's (BGCNAL) resources. User passwords must meet or exceed the following requirements:

1) Minimum password length = 12 characters
2) Not be the same as the User ID
3) Not be a dictionary word or proper name
4) Not be identical to the last 8 passwords
5) Must include three out of four characteristics: two CAPITAL Letters, two lower case letters, a number, a special character (e.g., !,@,#,$)

Please review the BGCA Password Policy (v2.0) for additional details BGCA Password Policies

F. Computer Equipment & Software Policy

The technology used to manage its information, operations and projects is a valuable asset of BGCNAL. The purpose of this policy is to protect these assets from unauthorized use, modification, destruction, or disclosure whether accidental or intentional.

BGCNAL provides approved, office-based or club-based full-time employees with a computer and the resources associated with its use for business communications including but not limited to e-mail, instant messaging, web and audio

conferencing, internet access, BGCA online applications and Websites, file sharing and voice mail. These systems and resources are the property of BGCA/BGCNAL and are provided to employees for business purposes.

The following policies and practices govern all BGCNAL Information Technology (IT) resources including computers, internal and external networks, purchased and custom software / applications, fax transmissions, telephone services, and peripheral devices.

The third-party Information Technology department, at the direction of the CEO, Human Resources and with the approval of the CEO or the Vice President, COO, will audit the use and contents of Information Technology resources. Special attention will be given to illegal or material that is inappropriate for the workplace; unauthorized software, applications, plugins, Browser extensions, or data; and malware. Any software, applications, plugins or extensions determined to be in violation of licensing agreements or not approved by Information Technology will be removed. Removal of this software may also remove personal data or images. Current end-point protection software (including, but not limited to anti-virus software) will be used to guard against the introduction of malicious software to the all BGCNAL environments.

Employees who discover non-compliance with these policies and practices must immediately inform appropriate management staff. Violations of the Information Technology policies and practices will be addressed as provided for in the Standards of Conduct section of the Employee Handbook.

G. Appropriate Uses of Technology

All BGCA employees are responsible for using information technology resources in an ethical, professional, and lawful manner at all times. The following are prohibited:

- Communications or actions that contain or convey sexually explicit materials, racial slurs, derogatory gender-specific comments, or any comments that offensively address someone's race, color, national origin, disability, sex, sexual orientation, gender identity or expression, age, religion, pregnancy, veteran or military status, genetic information, or any other protected group as specified by federal or state law.
- Viewing or storing pornography or any sexually explicit materials. Employees found with pornography or sexually explicit materials on BGCNAL equipment will be subject to discipline, up to and including termination of employment.
- Communications or actions which are abusive, threatening, defamatory, harassing or libelous.
- Commercial use or use which results in a personal financial gain.
- Attempting to gain unauthorized access to a computer system or network.
- Unauthorized access or alteration of another user’s data or programs.
- Use for outside organizations not authorized to use BGCNAL facilities.
- Use which violates the patent, copyright, trade secret, trademark, or other intellectual property right, privacy, or similar right of another party.
- Use which violates any governmental law, statute, ordinance, administrative order, rule, or regulation.
- Any violations of the above will result in disciplinary action, up to and including dismissal.

H. Use of BGCNAL Assets for Personal Use

BGCNAL recognizes that in this interconnected world, employees' work and personal lives need to balance out, and that it may be necessary to check personal email or visit a website for personal matters during the course of the day. BGCNAL does not generally restrict this access, and each employee needs to act responsibly and not let personal use impact their ability to perform their assigned job responsibilities. Supervisors need to be aware and ensure that BGCA information technology assets are being used appropriately. BGCNAL is not liable for any damage, edits/changes, or loss to personal data (e.g., financial, health, etc.) accessed via the Web or local files using BGCNAL IT assets.

I. Computer Security and Privacy

All computer software, software applications and data developed and/or processed by employees in the performance of their job or purchased for the use of BGCNAL belong exclusively to BGCNAL and may not be copied or removed without written authorization from the CEO, Third Party IT Support

Access to valuable and confidential BGCNAL information is limited to authorized users for approved purposes. Such authorized employees are trusted with this access and are responsible and accountable for appropriate use and protection from unauthorized modification, disclosure, distribution, or destruction.

BGCNAL and its Information Technology department do not offer individuals privacy protection in the use of its computers and software. Files and communications may be routinely monitored in line with procedures outlined above. BGCNAL may rightfully monitor or access any and all data, including internet usage and e-mail messages.

For further details on the Computer Equipment and Software Policy, please contact BGCNAL Information Technology.

J. General Email Usage

All correspondence that is sent from an employee of BGCNAL reflects on the Organization. Email provides a quick and efficient method of communication; however, overuse of email may result in an employee's inability to respond effectively, and sometimes it is better to call or communicate in person.

No user shall at any time send or store email that:

- would put any tangible or intangible company assets or property at risk
- is considered pornographic or adult in nature or would otherwise offend any person based on sex, race, religion, creed, or national origin
- involves hacking tools and techniques
- involves the violation of any copyright
- contains a warning about malware
- entices the recipient to click a link, open an attachment, or provide network login credentials or other sensitive information. Any such phishing emails shall be forwarded to IT staff for further review.
- contains unsolicited commercial email (spam) messages. All spam messages received shall be deleted immediately.

Refer to the General E-mail Usage and Guidelines of the Employee Handbook for more specific details on email usage guidelines.

K. Social Networking

As an employee, your online presence can impact BGCNAL's reputation. Be aware that your actions captured via images, posts, or comments may lead to disciplinary action, up to and including dismissal.

Personal blogs placed on social media networks or internet sites that contain or reference BGCNAL-related content should have clear disclaimers that the views expressed by the author in the blog are the author's alone and should not indicate in any way that they represent the views of BGCNAL. Be clear and write in first person. Make your writing clear that you are speaking for yourself and not on behalf of BGCNAL. Information published on your blog(s) related to work should comply with BGCNAL's confidentiality and disclosure of proprietary data policies. This also applies to comments posted on other blogs, forums, and social networking sites. Nothing in this policy shall be construed to prohibit employees from discussing the terms and conditions of employment or otherwise engaging in protected, concerted activities.

Please do not provide business references for current or prior employees on behalf of BGCA. See
Employment Verification and References. It is inappropriate to reference or cite BGCA's vendors, partners, or sponsors without express consent. Respect copyright laws, and reference or cite sources appropriately.

Plagiarism applies online as well. BGCNAL's intellectual property, logos and trademarks may not be used without written consent. See also BGCNAL's policy on Work Product Ownership.

All users of social media must remain aware of announcements made by Social Media providers regarding breaches to information such as personal or password information. Users must take immediate and appropriate actions based on the provider's recommendations to ensure that their social media account is secure. A compromised account could result in damage to use reputation or to that of BGCNAL and the greater Movement.

L. Protecting Confidential Information

- Protecting BGCNAL's business secrets and other confidential information is the responsibility of every employee, and all share a common interest in making sure it is not improperly or accidentally disclosed. Do not discuss BGCNAL's confidential information, including financial data and other non-public proprietary information, with anyone who does not have a legitimate "need to know" or is not designated to handle confidential information. If you have any questions, please consult your supervisor.

- Nothing in this policy is intended to prohibit employees from making a disclosure if the disclosure is made in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney, and solely for the purpose of reporting or investigating a suspected violation of law; or is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal.

- Similarly, nothing in this policy shall be construed to prohibit employees from discussing the terms and conditions of their employment or otherwise engaging in protected, concerted activities.

Refer to the Data Sharing Policy located in the Employee Handbook for additional data protection measures and examples.

IV. Roles and Responsibilities

It is the responsibility of the individual computer user to ensure that this policy is adhered to. It is the role of management to ensure that this policy is enforced.

A. How Compliance will be measured

Network, computer, and web browser logs are subject to being monitored or reviewed. All software use is subject to being monitored for license/copyright purposes. In addition, management reserves the right to perform random inspections at any time.

B. Sanctions

- 1st violation – reminder of the policy and possible requirement to re-enroll in BGCA cybersecurity training.
- 2nd violation – warning and documented violation in HR file and requirement to re-enroll in BGCA cybersecurity training.
- 3rd violation – meeting with information security officer and employee's manager for formal review of security policy and discussion of why it's endangering company assets
- 4th violation – will be assessed on a case-by-case basis with the information security officer, employee's manager, HR or Legal to determine disciplinary action.

C. Review and Evaluation

Boys & Girls Clubs of North Alabama shall review, evaluate, and document the outcome of each of the following on a periodic basis:

- Effectiveness of this policy
- Maintenance costs of this policy to the business
- Impact of policy controls to the business
- Impact of policy on technical infrastructure requirements

In addition, this policy shall be revised as needed based on, but not limited to, any of the following:

- Significant security incidents that have occurred
- New vulnerabilities discovered during ongoing security assessments or annual audits
- Changes to the organizational structure
- Changes to the information technology infrastructure

D. Related Documents

- Incident Response Plan
- Password Policy
- Data Loss Prevention Policy