Beaconhouse Al Khaleej
International School Sharjah

Network Acceptable Use Policy

Introduction

Beaconhouse Al Khaleej International School network facilitates communication for the members of the school community or the persons associated with the school, provides a resource for gathering information, and supports the school's-learning environment.

Scope and Purpose of this Policy

BAKIS's private network is available to authorized users only. Network use is governed by this policy. This policy documents standards for appropriate and fair use of networking resources, protects user security and privacy, and assures school compliance with government laws.

In this document, the term *users* refer to anyone using BAKIS's network.

Appropriate Use

- Users are expected to cooperate with system administrators.
- User activity on the network must not prevent or inhibit others from accessing network resources or the Internet.
- Users must not use or provide tools that damage files or computers, compromise network security, or disable accounts.
- Users must not send obscene, defamatory, or threatening messages or in any way harass others. Information transmitted or published is to be representative of a school.
- Users must not violate school policies.
- Users must not misrepresent another user's identity.
- Users must not distribute copyrighted material without written consent of the copyright holder. Unless otherwise indicated by the author, users should assume that any material not created by themselves is copyrighted.
- Users must not attempt to undermine the security or integrity of the school network and must not attempt to gain unauthorized access. Users must not use any computer program or device to intercept or decode passwords or similar access- control information. Suspected security breaches or vulnerabilities should be reported immediately to IT Department.

Privacy

- User privacy is important to the school and is protected to the extent that is technically feasible and allowed by law. The school systems maintain a certain level of logging of network activities.
- The IT Department endeavors to maintain the integrity and proper functioning of the systems for the benefit of all users. In connection with this responsibility, designated IT may need to access or monitor parts of the system. All IT is to respect the privacy of personal communications encountered. However, if IT personnel, while involved in routine duties, encounter information that indicates that a crime or a breach of this policy may have been committed or is about to be committed, they are required to report the existence and source of this information to the proper school authorities.
- Searching and monitoring of computing resources and network activities may be authorized by the school administration. Authorization, including delegation if applicable, must be in writing, and must specify the information or communications to be examined.

Security

Our goal is to provide a secure environment for personal and institutional computing and communication. The following are a few practical applications of those principles:

Network

- The network is divided into several security zones separating the Internet and school's internal networks.
- Any device connected to the restricted security zones must be registered through IT Department. (gaining access to Wi-Fi etc)
- Internet Protocol (IP) addresses used on the school network are school property, are assigned by IT, and may only be used with permission. Every computer connected to the network must use a school supplied IP address.

Servers

- Servers are computers connected to the school network that provide services or storage to multiple users.
- Only persons designated by IT have physical access or administrative password access to centrally administered servers or equipment. Access to these facilities are not issued to any individual without the permission of IT.
- All servers connected to the school network must be registered as such with IT. System administrators must take steps to ensure that the servers are secure. IT performs periodic security audits of all servers connected to the school network.
- A school server found to be a security threat will be reported to the administrator of

that server as well as to IT. If necessary, the server will be disconnected until the problem is fixed.

Workstations

- A workstation is a computer connected to one of the school networks.
- Workstations connected to a school network must not be configured to allow access to that network from any other network or from off-campus without proper authorization from IT. Users requiring access to secure resources while away from their workstation may request a virtual private network (VPN) account from IT.

General-use Computers

- A general-use computer is any device designated to work in a lab or kiosk environment.
- General-use computers must comply with the policies for workstations.
- IT must approve and oversee the configuration and installation of any general-use computer connected to the network.
- General-use computers are not given access to secure network zones.

Blocking

- Blocking-software is maintained to protect users from encounters with inappropriate materials. However, this should not be construed as an endorsement of any site that is not blocked.
- Users may request an exception to the blocking policy by emailing to the IT department

User responsibility

- While IT takes steps to make the network secure, the user plays a very important role in maintaining security.
- Users are not permitted to share passwords with anyone. No one, including IT employees, is authorized to ask for a password. It is strongly suggested that all users protect their credentials.
- Users are not allowed to share their access to school systems without authorization from IT.
- Users should either log out or lock their screens when away from their computers for an extended period of time.
- Users are to report suspected intrusions or other inappropriate activity to IT.

Violations

- **First Incident.**
  When a user appears to have violated this policy and the user has not been implicated in prior incidents, he/she is furnished a copy of this policy and is asked to sign an "agreement to conform to policy" statement.
- **Repeated Violations.**
  Repeated or what IT deems as a major violation, is going to be referred to the respective Principal for disciplinary action.