AL ZUHOUR PRIVATE SCHOOL

Acceptable Use Policy (AUP)

JUNE, 2026

ICT & IT DEPARTMENT

Acceptable Use Policy

Overview:

This policy establishes the acceptable usage guidelines for all AL ZUHOUR PVT. SCHOOL-owned technology resources. These resources can include, but are not limited to, the following equipment:

- Computers
  - Desktop Computers, Mobile Devices, Servers, etc.
- Network Equipment
  - Switches, Routers, Network and Communications Cabling, Wall Plates, Wireless Antennas, Wireless Bridge Devices, Fiber Optic Lines, Fiber Optic Equipment, Firewall, Access Controller, PABX, Phones, etc.
- Audio/Video Equipment
  - Video Codecs, HDTVs, Document Cameras, Projectors, Security Cameras, Miscellaneous Cabling, Digital Cameras and Camcorders, Printers, Copiers, Fax Machines, etc.
- Software
  - Operating Systems, Application Software, etc.
- Resources
  - Group Drive File Storage, Email Accounts, Shared drive, etc.

This policy applies to all employees and other workers at AL ZUHOUR PVT. SCHOOL, including all personnel affiliated with third parties, including vendors. This policy applies to all equipment that is owned or leased by AL ZUHOUR PVT. SCHOOL.

Policy:

While AL ZUHOUR PVT. SCHOOL's IT Department desires to provide a reasonable level of freedom and privacy, users should be aware that all AL ZUHOUR PVT. SCHOOL-owned equipment, network infrastructure, and software applications are the property of AL ZUHOUR PVT. SCHOOL and therefore are to be used for official use only. Also, all data residing on AL ZUHOUR PVT. SCHOOL-owned equipment is also the property AL ZUHOUR PVT. SCHOOL and therefore, should be treated as such, and protected from unauthorized access.

The following activities provide a general roadmap to use AL ZUHOUR PVT. SCHOOL's technology resources in an acceptable manner:

- All passwords used to access AL ZUHOUR PVT. SCHOOL systems must be kept secure and protected from unauthorized use.
- No user account can be shared between individuals. Authorized users are responsible for the security of their own passwords and accounts.
- Do not transfer personally identifiable information on portable equipment and storage devices.
- Public postings by employees from a AL ZUHOUR PVT. SCHOOL email address should contain the following disclaimer stating that the opinions expressed are strictly their own and not necessarily those of AL ZUHOUR PVT. SCHOOL, unless the posting is during business duties:
- Any views or opinions presented in this message are solely those of the author and do not necessarily represent those of Al Zuhour Pvt. School.
- Employees of AL ZUHOUR are expressly required not to make defamatory statements and not to infringe or authorize any infringement of copyright or any other legal right by electronic communications. Any such communication is contrary to AL ZUHOUR PVT. SCHOOL policy and outside the scope of the employment of the individual concerned.
- AL ZUHOUR PVT. SCHOOL will not accept any liability in respect of such communication, and the employee responsible will be personally liable for any damages or other liability arising.
- All computers residing on the internal AL ZUHOUR PVT. SCHOOL network, whether owned by the employee or AL ZUHOUR PVT. SCHOOL, shall be continually executing approved virus-scanning software with a current, up-to- date virus database.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders.
- Personally, identifiable information cannot be sent via electronic means and should be transferred within the internal network.
- All workstations should be kept secure. Users should lock the workstation when not attended to protect unauthorized users from accessing secure files.

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of AL ZUHOUR PVT. SCHOOL authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing AL ZUHOUR PVT. SCHOOL-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by AL ZUHOUR PVT. SCHOOL.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which AL ZUHOUR PVT. SCHOOL or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to the export of any material that is in question.
- Introduction of malicious programs into the network or server environments (e.g., viruses, worms, Trojan horses, rootkit, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using an AL ZUHOUR PVT. SCHOOL computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any AL ZUHOUR PVT. SCHOOL account.

- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.
- For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to the AL ZUHOUR PVT. SCHOOL IT Department is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within AL ZUHOUR PVT. SCHOOL's networks of other Internet/Intranet/Extranet providers on behalf of, or to advertise, any service hosted by AL ZUHOUR PVT. SCHOOL or connected via AL ZUHOUR PVT. SCHOOL's network.