

The Assam Valley School

'AVS IT PROTOCOL': - Computer, LED Panel & Internet Acceptable Use Agreement

This policy applies to all users of IT resources at The Assam Valley School, including pupils, staff, and visitors. All users must acknowledge and comply with this agreement before accessing the school's IT systems.

The Assam Valley School is committed to integrating advanced technology and providing enhanced access to learning opportunities. This policy aims to enrich education while ensuring the ethical, secure, and effective use of digital resources.

Any activity deemed inappropriate by the school is prohibited, even though not set forth herein.

1. ACCEPTABLE USE:

The purpose of the Internet is to facilitate communication in support of research and education by providing access to unique resources and an opportunity for collaborative work. To remain eligible as a user, all Internet use must be in support of and consistent with the educational objectives of the school. All users of the Internet must comply with existing rules and Acceptable Use Policies which are incorporated in this document.

Playing music, computer games, and chatting during academic/prep hours is not considered educational; they take up bandwidth on our network and therefore are not allowed. Deliberately running programs that "hog" bandwidth is not permitted.

2. PRIVILEGE:

The use of Computers/LED Panels/Internet is a privilege, not a right. Inappropriate use, including any violation of these conditions and rules, may result in cancellation of the privilege. AVS, under this agreement, is delegated the authority to determine appropriate use and may deny, revoke or suspend any use of the Internet at any time based upon the determination of inappropriate use by a user.

3. MONITORING:

Every staff and pupil at AVS will be allocated an official email account and the AVS Systems Administrator reserves the right to intercept, detain and read both incoming and outgoing e-mail and Internet traffic from the official account.

- a) Users are prohibited from transmitting or forwarding fraudulent, harassing or obscene messages or files. Accessing weaponry/bomb-making sites, sites of sexual content, gambling, or any other site(s) deemed inappropriate by the School is prohibited.
- b) Users are prohibited from transmitting or forwarding chain letters, mass mailings, MMS or 'SPAMMING'. Use of ANY e-mail programme or Internet accessibility programme by any user without the permission of AVS staff is prohibited.
- c) Any electronic mail or Internet access must be for AVS educational purposes only.

4. COMPUTER/LED PANEL/INTERNET ETIQUETTE:

All users are expected to abide by the generally-accepted rules of computer/network etiquette. These include, but are not limited, to the following:

- a) Be polite. Do not get abusive in your messages to others.
- b) Use appropriate language. Do not swear, use vulgarities or any other inappropriate language. Do not engage in activities which are prohibited under the law.
- c) Do not reveal your personal address, phone number, user credentials, credit card numbers or those of other pupils or colleagues.
- d) Students are prohibited from sharing personal images, videos, or information on online platforms without explicit permission from a teacher or guardian.
- e) Teachers and tutors must responsibly guide students' digital activities to ensure their safety without infringing on their privacy unnecessarily.
- f) Cyberbullying, harassment, or sharing explicit content via school IT systems is strictly forbidden.

- g) Email is not private. Users who operate the system do have access to all mail. Messages relating to or in support of illegal activities will be reported to the authorities and will result in the loss of user privileges. It is also possible that other penalties may be invoked.
- h) Do not use the Internet in such a way that you disrupt the use of the network by other users.
- i) All communications and information accessible via the Internet should be assumed to be the private property of the user who put it on the network.
- j) Eating or drinking is not allowed at any computer workstation or in any computer lab at any time.
- k) Network printers should be used responsibly to prevent waste and abuse.
- l) The LED Panels shall be used only for academic and school-related purposes.
- m) Inappropriate or unauthorized use of the panels will lead to disciplinary action in accordance with school regulations.

5.NO WARRANTIES:

AVS makes no warranty of any kind, whether expressed or implied, for the service it is providing. AVS **WILL NOT** be responsible for any damages a user suffers. This includes loss of data resulting from delay, no-deliveries, mis-deliveries or server interruptions caused by AVS or by the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. AVS specifically denies any responsibility for the accuracy or quality of information obtained through its server. All users need to consider the source of the information they obtain and consider how valid that information might be. AVS will not be held responsible for any damage of laptops.

6. SECURITY AND UNAUTHORIZED ACCESS TO FILES AND DIRECTORIES:

As AVS account holders, all the staff and pupils are owners of their data, and it is their responsibility to ensure that it is adequately protected against unauthorized access. To this end, users should keep their account password confidential. A user must never allow others to use his/her password. Users must use strong passwords to protect their accounts, ensuring system security, safeguarding their privileges, and maintaining uninterrupted access to the system.

Every user using the School Network must not engage in any activity intended to circumvent computer security controls. This means they must not attempt to crack passwords, discover unprotected files, decode encrypted files, **or engage in similar unauthorized activities**. This also includes creating, modifying, or executing programs that are designed to hack computer systems.

Attempts to bypass security protocols or log onto the Internet as a Systems Administrator will result in the cancellation of a user's privileges.

Users must install licensed antivirus software on their devices and ensure it is updated regularly to maintain system security and protect against threats.

If you feel you can identify a security problem on the Internet, you must notify the Systems Administrator. Do not demonstrate the problem to other users.

Any user identified as a security risk for having a history of problems with other computer systems may be denied access to the Internet by AVS.

7.UNAUTHORIZED USE OF SOFTWARE:

- a) Users are prohibited from loading, downloading, or copying any software on any computer system without approval from the Systems Administrator.
- b) Users are prohibited from downloading, possessing, using access to the school's computer system, or disrupting the computing processes in any way. Using viruses or any other invasive software is expressly forbidden.

8. VANDALISM AND HARASSMENT:

Vandalism and harassment will result in cancellation of user privileges.

Vandalism is defined as any malicious attempt to harm, modify and destroy any components of the machines, destroy data of another user, Internet or other network. This includes, but is not limited to, the introduction of viruses.

Harassment is defined as the persistent annoyance of another user or the interference of another user's work.

Harassment includes, but is not limited to, the sending of unwanted mail.

9. Social Media Policy:

Staff and pupils must represent the school positively on social media platforms.

Sharing sensitive school-related content without prior authorization is strictly prohibited.

10. ChatGPT Policy:

- a. AI tools should be used strictly for educational and academic enhancement purposes.
- b. Users must comply with all school regulations, cybersecurity practices, and academic integrity standards while using AI platforms.
- c. AI should be used to support learning and understanding, and not as a substitute for independent thinking, creativity, or personal effort.
- d. Plagiarism, direct submission of AI-generated assignments, or presenting AI-generated work as original work may result in disciplinary action.
- e. Uploading or sharing confidential school documents, personal records, financial information, passwords, or any sensitive data on AI platforms is strictly prohibited.
- f. Official school email IDs should be used wherever authorized and permitted by the school administration.
- g. Creating, sharing, or generating harmful, offensive, misleading, inappropriate, or unethical content using AI tools may lead to disciplinary action by the school authorities.
- h. All activities performed using school-owned devices, systems, or networks may be monitored, reviewed, and audited by the school administration at any time.

11. ENCOUNTER OF CONTROVERSIAL MATERIALS:

Users may encounter material which is controversial and which users, parents, teachers or administrators may consider inappropriate or offensive. However, on the Internet, it is impossible to control the content of data and a user may discover controversial materials. It is the user's responsibility not to initiate access to such material. If such material is inadvertently encountered, the link to it must be terminated immediately. AVS will not be held liable for any decision to restrict or regulate access to Internet materials.

12. REPORTING AND RESOLUTION MECHANISMS

Staff and pupils should report misuse, inappropriate materials, or security issues to the Systems Administrator or designated staff through email or a dedicated online form.

Any suspected violation of the POCSO Act must be reported immediately to the designated Child Protection Officer (CPO) of the school.

AVS will address these issues with appropriate disciplinary measures.

13. PENALTIES FOR IMPROPER USE:

With the first offence the pupil will lose the right to access the Internet and/ or use of computers/laptops for a week.

Succeeding offences will result in suspension from use of technology for increasingly longer periods up to the remainder of the semester or the school year. Permanent suspension may result in grave circumstances.

Extreme misuse of the Internet may result in expulsion for all users.

A list of pupils who have been denied Internet access will be published and distributed to the administration and teaching staff of AVS on a regular basis.

In addition, pursuant to IT ACT 2008 amendment, any unauthorized Internet access, attempted access or use of any computing and/or network systems which is in violation of national laws and/or other applicable laws is subject to criminal prosecution

14. HARDWARE/SOFTWARE:

All hardware and software are the properties of AVS and should not be moved or altered without the consent of the Systems Administrator.



Dr. Amit Jugran

Headmaster

The Assam Valley School

HEADMASTER
The Assam Valley School