AMITY
PRIVATE SCHOOL
SHARJAH

# IT Infrastructure Policy

| | |
|---|---|
| **Reference number** | APS – IT Infrastructure Policy/ 2021/04/14 |
| **Version** | Version 01 |
| **Review Schedule** | Annual |
| **Target audience** | All Stakeholders of Amity Private School, Sharjah |
| **Ratified by** | Ms. Bandana Lazarus<br>Principal |
| **Ratified date** | *April 2021* |
| **Reviewed by** | Mr. Nithin Thomas<br>Head of Information Technology, Amity Corporate |
| **Last Review date** | April-2021 |

## Content

## Introduction

APS Sharjah has the responsibility to ensure that every student in its care is safe whether in the digital world or the real world. The school is aware that IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods. New technologies are continually enhancing communication, the sharing of information and learning, social interaction and leisure activities.

However, we are also alert to the fact that they also pose great and more subtle risks to young people. Our students are, therefore, taught how to stay safe in the online environment and how to avoid risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalization.

## 1. Objective

- This policy, supported by the Acceptable Use policy for all staff, students, parents and visitors is implemented to protect the interests and safety of the whole school community.
- To provide clear guidance on how to minimize risks and how to deal with any infringements. All users need to be aware of the range of risks associated with the use of these internet technologies.
- To educate our students on E-Safety issues to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom.
- To engage students in discussions about E-Safety and listening to their fears and anxieties.

## 2. Scope of this Policy

This policy applies to all members of the school community, including staff, students, parents and visitors, who have access to and are users of the school IT systems.

**Staff** includes teaching and non-teaching staff and regular volunteers.

**Parents** includes students' caregivers and guardians.

**Visitors** includes anyone who is visiting the school, including occasional volunteers.

The Infrastructure policy along with Acceptable Use Policy for all staff and students, cover both fixed and mobile internet devices provided by the school such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc. as well as all devices owned by students, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

## 3. Roles and Responsibilities

### 3.1. The Principal

- The Principal is responsible for the approval of this policy and for reviewing its effectiveness. The Policy is to be reviewed every year in light of changes in technology.
- To ensure that staff are aware of and follow the school E-Safety policy and procedures.

### 3.2. Students

- Students are responsible for using the school IT systems in accordance with the E-Safety policy.
- Students have understood the E-Safety protocols.

### 3.3. Parents

- Parents to be fully engaged in promoting E-Safety both in and outside of school. Parents to support the school for endorsing the school's E-Safety policy and other relevant policies related to safeguarding
- Parents to promote a wide understanding of the benefits and risks related to internet usage.

## 4. Education and Training

### 4.1. Staff – awareness and training

- New staff receives information on the School’s E-Safety policies as part of their induction.
- All staff receive regular information and training on E-Safety issues through internal training and meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of E-Safety.
- All staff working with children are responsible for demonstrating, promoting and supporting safe behaviors in their classrooms and following school E-Safety procedures.
- Teaching staff are encouraged to incorporate E-Safety activities and awareness within their subject areas and through a culture of talking about issues as they arise.
- When children are using school computers, staff make sure children are fully aware and are following the school's IT guidelines.
- Staff understands what to do in the event of misuse of technology by any member of the school community.
- The school staff understands their responsibilities to report onlinE-Safety incidents.
- The school encourages all users to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school’s escalation processes; Incident report flow chart is in place and understood so that processes are followed promptly.
- The school has the provision to seek support from other outside agencies in dealing with onlinE-Safety issues in case there is a need.

### 4.2. Students

- IT and online resources are used increasingly across the curriculum. The school provides guidance to students about E-Safety within a range of curriculum areas and IT lessons and through presentations, workshops, assemblies on a regular and meaningful basis. The school continuously monitors and assesses students’ understanding of it.

- At age-appropriate levels, students are taught about their E-Safety responsibilities and to look after their own onlinE-Safety risks (including recognizing online exploitation, stalking and grooming), and of their responsibility to report any such instances they or their peers come across.
- The school encourages all users to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes. Incident report flow chart is in place and understood so that processes are followed promptly.
- Students are taught about respecting other people's information and images.
- Students are aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy).

### 4.3. Parents

- The school seeks to work closely with parents in promoting a culture of E-Safety.
- The school contacts parents if it has any safety concerns about students' behavior while using technology online. Parents are guided and informed likewise to share any concerns, which they identify with the school.
- The school arranges training sessions/workshops for parents advising them about E-Safety and the practical steps that they can take to minimize the potential dangers to their ward, without curbing their natural enthusiasm and curiosity. These are done by both in-house trainers and specialist from outside.

## 5. Policy Statements

### 5.1. Password Security

- Staff have individual school network logins and storage folders on the Cloud.
- Staff and students are regularly reminded of the need for password security. All students and members of staff are advised:
  - to use a strong password usually containing eight characters or more and containing upper and lower case letters as well as numbers,
  - not to write passwords down and
  - not to share passwords with other students or staff.

### 5.2. Password Aging

- User passwords must be changed every 3 months. Previously used passwords may not be reused.

### 5.3. Password Protection

- Passwords must not be shared with anyone (including coworkers and supervisors), and must not be revealed or sent electronically.

- Passwords shall not be written down or physically stored anywhere in the office.
- When configuring password "hints," do not hint at the format of your password (e.g., "xyz + middle name")
- User IDs and passwords must not be scripted to enable automatic login.
- "Remember Password" feature on websites and applications should not be used.

### 5.4. Enforcement

- It is the responsibility of the end user to ensure enforcement with the policies above.
- If password may have been compromised, the incident is to be immediately reported to itsupport@amitysharjah.ae and password needs to be changed.

## 6. Filtering Policy

- It is important to note, that any filtering service, no matter how thorough, can never be comprehensive. Therefore the school has a clearly understood policy on acceptable use for all users and adequate supervision is maintained.
- The schools Wi-Fi and infrastructure has been installed and is maintained with an active, monitored filter system to satisfy both the needs of child protection/inappropriate content whilst ensuring that it serves to support teaching and learning.
- If at any time school staff or students find themselves able to access internet sites from within school which they think should be blocked, they are advised to report the matter to a member of the EST (E-Safety Team). The IT manager will implement agreed procedures for handling such issues.

### 6.1. System

The network is protected through a Firewall (Cyberoam 100ing) and relevant policies are enabled to protect the IT usage and infrastructure.

### 6.2. Cyberoam 100ing Provision

Cyberoam 100ing provides an effective filtering system, because of which the following categories of websites are not, by default, available to school users:

- Adult: content containing sexually explicit images, video or text, the depiction of actual or realistic sexual activity.
- Violence: content containing graphically violent images, video or text.
- Hate Material: content, which promotes violence or attack on individuals or institutions based on religious, racial or gender grounds.
- Illegal drug taking and the promotion of illegal drug use: content relating to the use or promotion of illegal drugs or misuse of prescription drugs.
- Criminal skill/activity: content relating to the promotion of criminal and other activities.

- Gambling: content relating to the use of online gambling websites or information relating to the promotion of gambling and gambling advice.

### 6.3. Access to Network

Access to the network is provided through Radius Authentication. Access is therefore governed by device registration and approval by authorized staff only. No devices can join the network without this approval and authentication.

### 6.4. Hardware and General Service Provision

The following has been installed and configured in school to ensure only appropriate content is available to all users;

- School licenses are purchased on a fixed three year term to ensure continuity of service and the individual firewall is monitored 24/7 with instant notification of any concerns.
- A hardware firewall filter is installed which intercepts all Internet traffic leaving and entering the school network and this cannot be circumvented.
- The firewall appliance is configured for the Global view Internet filtering service, powered by Cyberoam. The service is a professional, commercial category based web-filtering solution and is used in many organizations worldwide.
- It uses a category-based system to group web sites in addition to keyword, IP and specific white and blacklist control.
- In addition, IP and URL black and white listing is supported locally which ensures any content that is flagged as non-desirable on the network, can be disabled immediately.
- Full access logs are maintained for all traffic and all attempts at access of inappropriate content.

### 6.5. Specifics of Filtering Service

- Cyberoam independently searches the Internet using their tools to select what category is assigned to any available website. This is matched to the live filtering within the school
- If a website falls into a category that is not deemed acceptable for use in the classroom, the user gets an “unsuitable” notification on the web browser and this activity is logged to user and device level.
- Filtration service uses a category-based system to decide if a website is viewable from all Internet connected devices. The primary Categories include
  - Computer & Internet Services (spam sites)
  - Child Protection (including child sexual abuse; extreme pornography or criminally racist or terrorist content)
  - Other (dating and person)

## 7. Technical Security

### 7.1. Objectives

- To detect, prevent and minimize the impact of Virus outbreaks in the organization's systems such as, servers and user-end desktops & laptops.
- To protect the systems against the spread of malicious viruses.
- To define appropriate control measures for users in order to protect the systems against virus attacks.
- To ensure the protective and optimum performance of the users when using the systems without any considerable delays.

### 7.2. Software: McAfee

### 7.3. Anti-Virus Policy

The school follows the below preventive and detective control measures to protect against malicious software and virus attacks;

- Scanning for Viruses.
- Users are allowed to use only authorized/licensed software in the school or while using the school intranet. Use of any other software without the permission the IT manager and the EST of the concerned department is prohibited.
- All files and software downloaded/received either from or via external networks, e-mail, or on any other medium such as data storage media should be first scanned for viruses/ malicious code prior to its use.
- Database/file servers where critical data is stored is scanned for viruses on a regular basis.
- Any data storage media brought into the organization must be scanned for virus before being used by the user or to be given to the Information Security Team for scanning.
- School Laptops for users are first updated with the Anti-virus software and scanned for viruses by the information security team and approved, before connecting to the School network.

### 7.4. Desktop & Laptop Usage Policy

### 7.4.1. Objectives

- To ensure the acceptable use of the school information systems such as desktop and laptop.
- To ensure that employees follow an appropriate level of responsibility to safeguard the desktop and laptop that they have been allocated.
- To ensure that if a laptop is lost or stolen, the only impact to the organization is the loss of the physical laptop asset value and not the valuable information residing on it.
- Desktops and Laptops are issued to the user only after the approval/authorization by the Manager of the concerned department.

- The Desktop and Laptop is withdrawn when the employee leaves the school and/ or if a user's contract comes to an end or upon a request from the Manager of the concerned department.

### 7.4.2. Statements

- Users must safeguard their Desktop/Laptop against loss, theft or damage.
- Users must lock their account when leaving the Desktop and/or Laptop unattended.
- Users must take care to safeguard Information Assets when accessing the IT Infrastructure from a public place.
- Users must adhere to the approved organization's encryption policy when storing sensitive and confidential information on their Laptop.
- Users must backup their business related files that they store on their Desktop and/or laptop on a regular basis on their Cloud backup folder.
- Users must not tamper with the Administrative functions of the Desktop and/or Laptop such as its Operating System or Administrator identification and password.
- Users must use the school request and approval procedures for requesting the installation of external devices such as printers, storage devices, and third party software to their Desktop and/or Laptop.

### 7.4.3. Terms and Compliance

- All users are responsible to safeguard the Desktop/Laptop issued to them and any stored Information Assets on it.
- In the event of loss of a Laptop, users must report the loss to IT manager at school immediately, in order to limit the access to school systems.
- The IT team must investigate the circumstances of the loss of a Laptop before a replacement is issued to the user.
- In case of non-compliance to this policy, disciplinary actions will be issued by the Information Technology division and reported to the Manager of the concerned department.

## 8. Use of Internet and Email

### 8.1. Staff

- Staff must not access any website or personal email, which is not connected with schoolwork or business whilst teaching / in front of students. Such access may only be made during Non-contact time with the students.
- Staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.
- The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses are monitored.

- Staff must immediately report to EST the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the IT Manager at school.
- Any online communications must not either knowingly or recklessly: ·
  - place a child or young person at risk of harm, or cause actual harm,
  - bring Amity Private School, Sharjah into disrepute,
  - breach confidentiality,
  - breach copyright;
  - breach data protection legislation,
  - be considered discriminatory against, or bullying or harassment of, any individual, for example: making offensive or derogatory comments relating to sex, gender reassignment, race, nationality, disability, sexual orientation, religion or belief or age;
  - use social media to bully another individual,
  - post links to or endorsing material which is discriminatory or offensive.
- School students should not be added as social network 'friends' or contacted through social media.
- Any digital communication between staff and students or parents must be professional in tone and content. Under no circumstances may staff contact a student or parent using their or any other personal email address.
- The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

### 8.2. Students

- The school network is protected via a strong anti-virus and firewall protection. Most spam emails and certain attachments are blocked automatically by the email system. Certain websites are automatically blocked by the school's filtering system.
- The school expects students to think carefully before they post any information online, or repost or endorse content created by other people. Content posted should not be deemed inappropriate or offensive, or likely to cause embarrassment to others.
- Students must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication to the EST.
- Students must report any accidental access to inappropriate materials directly to the school EST.
- Deliberate access to any inappropriate materials by a student will lead to the incident being recorded on their file and will be dealt with under the school's Behavior Management Policy.
- Students should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

## 9. Protecting Personal Data

- The school follows privileged access management methodologies by which the user gains access to only relevant information and access, which is required for them to do their duties.
- Staff can back up important Data in the PC with OneDrive folder backup, so that it is protected and can be recovered in the event of a data failure. A Data failures can be the result of hardware or software failure, data corruption, or a human-caused event, such as a malicious attack (virus or malware), or accidental deletion of data.

### 9.1. Digital Data Integrity, Management and Data Safeguarding

- Student/Staff related data must not be deleted from any system either local or in the cloud.
- Student/Staff data must not be shared with outsiders in any form unless the request is from a competent authority for legal proceedings. In such cases, written request from such competent authorities needs to be submitted in official channel which is approved by the Principal.
- Data must not be uploaded to any other web instances other than Sharjah Private Education Authority (SPEA) and Central Board of Secondary Education (CBSE) approved site/portal.
- SPEA/CBSE updating must only be through the designated computer/staff.
- All data maintained by staffs through joint or individual research/efforts are the intellectual property of Amity and hence the sole ownership rests with Amity.
- Staff when leaving Amity MUST handover the same to Principal/ Department Head and the same to be verified and confirmed to IT Department.

### 9.2. Data Storage and Processing

- Staff can back up important Data in the PC with OneDrive folder backup, so that it is protected and can be recovered in the event of a data failure.
- No personal data of staff or students should be stored on personal memory sticks.
- Any security breaches or attempts, loss of equipment and any unauthorized use or suspected misuse of IT must be immediately reported to the school EST.

### 9.3. Misuse

- Amity Private School, Sharjah does not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the appropriate authority.
- Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's policies and procedures in particular the Safeguarding Policy.
- The school will impose a range of sanctions on any student who misuses technology to bully, harass or abuse another student in line with our Anti-Bullying Policy.
- Prompt action will be taken if a member of staff, a student or a parent has a complaint or concern relating to E-Safety. Complaints should be addressed to the school EST in the first

instance, who will liaise with Senior Leadership, and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

- Incidents of or concerns around E-Safety will be recorded using an Incident Report form and reported to the school's Principal, in accordance with the relevant safety policy of the school

## 10. Acceptable Use Agreement – Policy

The school has Acceptable Use Agreement Policy for the school community members

- Staff
- Students
- Parent/Caregivers
- Visitor/user

## Monitoring and Review

| S. No. | Version | Description of Change | Date |
|---|---|---|---|
| 1. | 1.0 | Adoption of the Policy | April 2021 |

**Principal | Ms. Bandana Lazarus** :

**Vice Principal | Ms. Alka Yadav** : Alka

**Online Safety Leader | Ms. Saritha Ajailal** :