Tenby Schools, Tropicana Aman

Whole School Policy

Policy	TTA IT Acceptable Use Policy		
Approval Date	August 2022	**Next Review**	August 2023
Review Cycle	12 months		
Scope	**Whole Group**	☐	**Whole School**	√
	International Primary	☐	**International Secondary**	☐
Ownership	Tenby Schools, TTA	**Approved by**	TTA SLT

1. Applicability

This policy applies to officers, employees, students, interns, contractors, vendors and anyone else who uses or accesses the device, network or information systems at TTA.

Exceptions to this policy must be approved in writing by the Regional Head of Information Technology (South East Asia).

2. Registering Devices

All devices must be registered with the IT department at TTA.

3. Level of Access

The TTA IT Department reserves the right to determine the level of access for each device. A user could be granted full, partial or guest access. The TTA IT Department may install a digital certificate (or its equivalent) on each device, which will authenticate the user, where applicable.

4. Third-Party Applications on Devices

a) The TTA IT Department reserves the right to block or limit the use of any third-party application, including those that may probe the network or share files illegally or harm the systems or network of the school.

b) As the number of approved applications continually evolves, a user must check with the IT Department for the current list of approved third party applications and obtain the prior approval of the IT Department before downloading any application on the device.

5. Remote Wiping

The IT Department reserves the right to remotely wipe a device at any time. By doing so, not only will school or company data get wiped, but the user's personal data could also be lost as well. The user must understand and accept such risk.

6. User Responsibilities

a) Any user that wishes to access the network using the device may do so using only software and application approved by the IT Department.

b) A user must use a device responsibly including not do any of the following:
   i. Use the service to violate any laws
   ii. Break the security of any device or network
   iii. Send junk email or spam anyone
   iv. Send a substantial number of emails to any person or system to flood their device or the server of the school.

c) A user must adopt and follow good security practices and immediately report any security concerns to the IT Department including but not limited to the following:
   i. Password protect the device
   ii. Not leave the device unattended
   iii. Report if the device is lost or stolen
   iv. Report if the device has been attacked with malware, a virus or any other suspicious attack
   v. Report any other security concern with regards to data

7. Return of Device

The IT Department reserves the right to request for the device to be returned to the school. A user must immediately return the device upon receipt of such request, failing which the school or company may take appropriate action.

8. Amendment and Update

The IT Department reserves the right to amend and update this policy at any time and in any such event, will use reasonable efforts to notify all users.

9.   Release of Liability and Disclaimer

A user hereby acknowledges and accepts that the use of a device in connection with the school or company carries specific risks for which the user shall assume full responsibility and liability and the user shall release the school or company from any liability, loss, claim or expense to the maximum extent permissible under the laws of Malaysia.