Mahanaim: IT Policy

Mahanaim grants its students and its employees the rights and privilege of connecting their personal devices to out network. Mahanaim also reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of the data regarding the institution, its students and its employees as well as protecting our technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

Mahanaim students and employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to our network.

All connectivity will occur through the Mahanaim Network which students can access after registration with their Mahanaim credentials (email and network password) or pre-defined network password.

All software and apps required for successful completion of modules is available on the devices in the Mahanaim campus. Individuals may purchase software or apps privately to use on their personal devices; however, it is the individual's responsibility to ensure that the software is compatible with their device.

Students wishing to use comparable software or different versions than those in use at Mahanaim should check with their module leaders to ensure that the replacement software will allow the student to perform all necessary tasks.

Acceptable Use

- Mahanaim defines acceptable business use as the use of Information systems for the purpose of, learning, teaching research, engagement and administration.
- Mahanaim defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing.

- All software and access provided by Mahanaim must be used in accordance with the End User license agreements of those products. Violation of such licensing agreements will lead in termination of access.
- Devices may not be used at any time to:
    - Store or transmit illicit materials
    - Store or transmit proprietary information belonging to another company
    - Harass others
    - Conduct other activities which interfere with the school's ability to generate an academic and administrative environment that is productive, ethical, legal, secure, facilitative and effective
- In order to ensure that information systems function in a secure, efficient and effective manner, the school reserves the right to examine any information on its facilities and to monitor use.

Devices and Support

- Connectivity and network issues are supported by the IT Helpdesk; issues relating to personal hardware, laptops, tablets, or phones is the responsibility of the owner of that hardware.
- Software issues are the responsibility of the party owning the software license.

Security

- In order to prevent unauthorized access, all devices accessing the network and its resources must be password protected using the features of the device and a strong password is required to access the Mahanaim network.
- The device should be set to lock itself with a password or PIN if it's idle for five minutes.
- Access to Mahanaim data is limited based on user profiles defined by IT and automatically enforced.
- Mahanaim may remotely remove devices or deny access to the network or services if 1) a device is lost, 2) a student or employee terminates his or her enrollment or employment, 3) a data or policy breach, a virus or similar threat to the security of the school's data and technology infrastructure is detected.

Risks/Liabilities/Disclaimers

- While Mahanaim take every precaution to protect the security and integrity of their network, it is an individual's responsibility to take additional precautions, such as backing up email, contacts, documents, assignments, etc.
- Mahanaim reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to Mahanaim within 24 hours.
- The individual is expected to use his or her devices in an ethical manner at all times and adhere to the school's acceptable use policy as outlined above.
- The individual is personally liable for all costs associated with his or her device.
- The individual assumes full liability for risks including, but not limited to, the partial or complete loss of school and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.