AY 2020-2021

IT Acceptable Use Agreement

The following guidelines apply to all Users at the UWC Mahindra College of India who access the college network, Wi-Fi & wired internet, associated infrastructure and cloud services within the @muwci.net GSuite for Education; all collectively known as the **College IT Network**. Access and use of the College IT Network is encouraged where such use supports the goals and objectives of education and is in line with applicable local laws and campus norms. However, access to these resources is a privilege - not a right - which might be partially or fully revoked, either temporarily or permanently, if the User fails to adhere to the guidelines detailed in this Acceptable Use Agreement. All Users are required to acknowledge receipt and confirm that they have understood and agree to abide by the guidelines hereunder.

Key Usage Guidelines

RESPONSIBLE & MINDFUL USE Users must use the College IT Network responsibly and productively. Access is primarily for education-related activities, such as academic research and tasks that aid in intellectual and personal growth. Users are expected to develop the skills of using technology mindfully to maintain the balance between their digital and 'real' lives.

ADHERENCE TO COLLEGE POLICIES All pertinent College Policies (including the Discrimination & Sexual Harassment Policy, Anti-Ragging Policy, Confidentiality & Information Security Policy, as well as Educational Policies when relevant) apply to Users while using the College IT Network. Users should adhere to a high standard of behavior with respectful and ethical conduct and communication at all times. Any reported incident of harassment, vulgarity, fraud, etc. will be treated seriously in line with the college Disciplinary Policies.

NETWORK ACCESS PRIVILEGES: Users will be provided access to appropriate areas of the local network, intranet, GSuite for Education apps and the World Wide Web. Website access will be limited to content deemed appropriate for minors and may be subject to time and data limits. Restrictions will apply to content that is incompatible with our educational objectives, such as websites with content related to pornography, gaming, gambling or other malicious, illegal or unethical material.

NETWORK PROTOCOLS: Users should respect network security & usage protocols, such as firewalls and bandwidth caps, as outlined further on in this Agreement. Any attempt to tamper or bypass these protocols through unauthorized access, hacking, impersonation, VPNs, or equivalent will result in disciplinary action or suspension of privileges.

COPYRIGHT COMPLIANCE: Users must adhere to copyright laws and are prohibited from downloading, sharing, copying or pirating software and electronic files without authorization. Use of P2P and torrent software is strictly prohibited.

MALWARE PROTECTION: Users must not compromise the College IT Network by introducing malware on personal or College devices. Special attention is to be paid to the installation of unverified shareware and freeware. Users are required to have active and updated anti-virus protection for any personal device that is registered to access the College IT Network.

PRIVACY: The College will respect the privacy of data maintained on the College IT Network where it is possible to do so. Under certain circumstances it may be necessary for IT Staff or senior College administrators to view User data, if it is necessary to resolve a fault, investigate a breach of college rules or when legally required to disclose information to third parties, such as the Police. In using the Colleges IT Network, the User consents to the viewing or disclosure of data resulting from the use of these resources.

DATA & BACKUP Though the IT Department regularly backs up institutional data on the College IT Network, it is not responsible for backing up User data stored on College-owned or personal devices or for the cost of retrieving data in the event of machine failure or loss. Users should plan to take periodic backups of their own data.

CONFIDENTIALITY, SECURITY & AUTHORIZED USAGE: Users should never share their confidential passwords for login access with anyone else. Users are responsible for protecting their accounts (e.g. by signing out of all services on public computers or securing private computers with master passwords) and will be held accountable for all actions undertaken by anyone else using their account. Similarly, unauthorized attempts to gain privileged access or access to any account or system not belonging to a User on the College IT Network will be treated seriously in line with the College Disciplinary Policies. Users must agree to never share confidential or proprietary information about the College and its constituents (students, faculty/staff, alumni and supporters) without written authorization.

Use of Fixed IT Assets

College IT Assets include any computers owned or maintained by the college, along with any peripherals or associated hardware such as printers, scanners, projectors, AV equipment, keyboards, mice, UPS backup devices and cables, along with any software installed. It also includes any networking hardware such as switches, access point hubs and network ports along with any internet connections or hardware that the college operates. IT assets are spread across campus in classrooms, auditoriums, offices and dedicated Computing Labs (IT Center Lab, Digi Lab). Rules for usage are as follows:

- IT Assets must be used responsibly and all equipment must be treated with care & respect.
- Users encountering issues with IT Assets should promptly report the same to it@muwci.net so the issue can be flagged and rectified for the next/other Users.
- Any instances of tampering, removal or damage of IT assets will be treated in line with the College Disciplinary Policies.
- A quiet working environment must be maintained in public Computing Labs.
- No food or beverages should be brought near IT equipment.
- Printing facilities provided in Computing Labs must be used in moderation and with due consideration for the environment.
- All ***Key Usage Guidelines*** (detailed overleaf) are applicable when using college-owned IT assets, especially protecting public computers from malware; adhering to secure account login and password protection protocols; and remaining mindful of limitations around personal data and privacy on shared computers.

Use of Personal Devices

The use of personal devices is permitted as per the following guidelines:

- **Device Limit:** Students may register no more than 3 personal devices for use on the College IT Network, including a laptop (mandatory), mobile phone (recommended) and an optional third device like a tablet/e-reader/iPod etc. Students with full scholarship support who are unable to procure a laptop may request the Admissions Office for a laptop on loan during the duration of their programme.

- **Types of Devices**: Any additional internet-connected devices (e.g. smart home devices, gaming consoles etc.) are not permitted and against our principles on the mindful use of technology. (see ***Key Usage Guidelines*** around *Responsible & Mindful Use*)
- **Software Requirements**: Personal devices must be malware-free and not have any P2P clients or unlicensed software installed on them. The IT Department provides free virus protection software to Users, who are then responsible for keeping these protections up-to-date.
- **Device Protection**: Users must take full responsibility for all repairs or replacements of their personal devices. It is recommended to use high quality plug adaptors and surge protectors while charging personal devices. Users must also take special precautions to protect their devices against theft.

Use of the Internet & Cloud-Based IT Assets

Users are offered access to the World Wide Web after registration on the College Wi-Fi network via the IT Department. While the internet can be a highly useful educational tool, Users must keep the following guidelines in mind:

- **Bandwidth Usage**: The College bears a significant cost to provide a high speed connection in our remote location. Accordingly, usage is monitored for each individual User and must not exceed 3GB per day. Bandwidth caps or blocks are enforceable when a User is in violation of this policy.
- **Cloud-Based Services**: Students also have access to a range of cloud-based services to support their learning programme, which they should fully familiarize themselves with. These include: GSuite for Education Suites (including @muwci.net email, College Intranet & Google Classroom); Managebac IB Learning Platform for curriculum planning, assessment & reporting; Online Educational Services for Curriculum, Research and University Guidance; Local Cloud Storage (Network Attached Storage at upto 20GB per User).
- **Inappropriate or Illegal Content**: Content filters are enforced on the unregulated resource of the world wide web to uphold UWC values and meet legal requirements related to copyright and child safeguarding. Since these tools do not provide 100% protection against misuse or inappropriate content, Users must practice additional self-regulation to guard from personal risk and legal liability.
- **E-Safety Education:** The College will provide opportunities to educate Users on safe and effective ways of using digital and electronic technology. Users must be aware of the dangers associated with being online such as privacy risks, hacking, cyber-bullying and online predators, amongst others. Whilst governing one's own actions, Users must also report inappropriate or unsafe digital interactions they witness as a bystander, especially where such actions could bring harm to the individual, cause harm to others or damage the reputation of the College. Users perpetrating any unethical online behaviors themselves will be faced with College Disciplinary Procedures (see ***Key Usage Guidelines*** around *Adherence to College Policies*)
- **Social Media:** Users are encouraged to use social media thoughtfully, constructively and in line with the College's Key Usage Guidelines. Users must ensure that when using social media for personal purposes they do no harm to the College's reputation or themselves.

Email & Communication

Every User is allotted a unique GSuite for Education login, which includes access to an @muwci.net Gmail account. Usage guidelines are as follows:

- **Email Usage**: Users can expect to receive and send regular communication to individuals or relevant groups/mailing lists via this service. Even if a User has an independent email address, they must check the College issued account regularly for key instructions and updates.
- **Communication Guidelines:** While using College email, Users are acting as representatives of the College and must adhere to a high standard of online conduct. In addition, Users are expected to observe good email etiquette such as timely responses, concise but polite presentation, informative subject lines, thoughtful assignment of recipients, appropriate use of attachments, maintaining privacy and avoiding spam, malware & copyright infringement.
- **Communication with Faculty/Staff:** All digital communications between faculty/staff and students must be professional at all times. Online communication with faculty/staff or other adults associated with the college is restricted to College-provided services like email or Managebac.
- **Account Suspension:** Cloud-based services including email account privileges will be available to Users only for the duration of their enrollment at the College. Users are responsible for backing up and saving their information before losing account access as per the following schedule:
    - Students-
        1. *Graduating students*: account suspension within 5 months (i.e. by 31st October for each graduating class).
        2. *Gap year students*: contact the Deputy Head of College and/or Guidance Office to request an extension of the 31st October cut-off date (for a maximum period of 1 year, i.e. till 31st May of the following year).
        3. *Expulsion / Withdrawal*: account suspension within 1 week.
    - Staff-
        1. Account suspension within 3 months of their last working date.
        2. Account suspension with immediate effect in case of termination.
    - Faculty-
        1. Account suspension within 3 months of their contract end date.
        2. Account suspension with immediate effect in case of termination.

IT Department Contact

Access to school computing facilities is managed by the IT Department, which can be contacted at the one point email ID it@muwci.net. If an user is unsure about what constitutes acceptable usage, then they should contact the IT Department for further clarifications.