T. A. Marryshow Community College

INCIPIENTES STATU PRESENTI USQUE AD TERMINUM QUORSUM IMUS

Laptop Usage Policy

This policy outlines the responsibilities that The T. A. Marryshow Community College Faculty and Staff must accept when they are issued a laptop computer.

Who is affected by this policy?

This policy applies to Faculty and Staff of the T. A. Marryshow Community College who have been issued a laptop by the College.

Why was this policy created?

Laptops provide the convenience of portability. This convenience exposes the College to certain risks. These include, but are not limited to:

- Theft of College property - laptops are easy to steal and their relatively high value and easiness to sell makes them common targets of theft.
- Exposure of sensitive information - misplaced or unsecured laptops may expose sensitive information to the public.
- Damage of College property - laptops are more susceptible to damage, both due to their portable nature and their relatively fragile construction.

What do I need to do?

If you are issued a laptop, you must sign a copy of the T. A. Marryshow Community College Laptop Usage Policy upon receipt. The signed copy of the policy will be kept at the IT Department or other designated area of the College until the laptop is returned or replaced. A link to the policy will also be posted on the College Policies and Guidelines webpage.

T. A. Marryshow Community College Laptop Usage Policy - Content

When a T. A. Marryshow Community College Faculty or Staff member is provided with a laptop, he/she accepts responsibility for safeguarding the laptop itself as well as the data stored on the laptop.

A. Intended Use of Laptops

Laptops and its related accessories shall be the property of the T. A. Marryshow Community College at all times and the employee will not have any right or interest in the said asset except using such asset during the employment or for such duration as may be decided by the College.

B. Laptop Security Controls

All laptops acquired for employees on behalf of the College shall be deemed to be the property of the College. Each employee issued with a laptop shall be responsible for the security of that laptop, regardless of whether the laptop is used in the office, at the employee's place of residence, or in any other location such as a hotel, conference room, car or airport. Employee shall ensure security of the laptop in each of the following domains as per the stated guidelines. Laptops must compulsorily be protected by a username and password.

C. Physical Security & Theft Prevention

To ensure physical security of laptops and data therein, all employees are required to undertake the following actions:

1. The physical security of the College provided laptops is the employee's personal responsibility. He/she is therefore required to take all reasonable precautions, be sensible and stay alert to the risks.

2. Keep your laptop in your possession and within sight whenever possible, just as if it were your wallet, handbag or mobile phone. Be extra careful in public places such as airports, railway stations or restaurants. It takes thieves just a fraction of a second to steal an unattended laptop.
3. Never leave the laptop unattended when using it outside the office.
4. Lock the laptop away out of sight when you are not using it, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office or in a hotel.
5. Never leave a laptop visibly unattended in a vehicle. If necessary, lock it out of sight in the trunk or glove box but it is generally much safer to take it with you. (Do note: Excessive temperatures can damage a laptop).
6. Carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage.
7. Employees may not take the laptop for repair to any external agency or vendor at any point of time.
8. In case of any failure, employees are required to report the same to the the IT Department.
9. (In the case of stolen laptop, the employee to alert the I.T. Department immediately. Report to be sent by email to helpdesk@tamcc.edu.gd.
10. The College maintains the right to conduct inspections of any computer equipment, including all laptop it owns or manages without prior notice to the Employee who is at the time the user or custodian of such computer equipment.
11. In case of leaving the employment or being terminated for any reason, employee will hand over the asset to the College in good condition failing which the College is authorized to charge penalty against the employee.

D. Data Security Controls

Employees are expected to ensure the security of the data within their laptops. In this regard you are to adhere to the following:

1. You are personally accountable for all network and systems access under your user ID, so keep your password absolutely secret. Never share it with anyone, not even members of your family, friends, or IT staff.
2. The College laptops are provided for official use for authorized employees. Do not loan your laptop or allow it to be used by others such as family and friends.
3. Avoid leaving your laptop unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before walking away from the machine.

E. Virus Protection

1. Email attachments are now the number one source of computer viruses. Avoid opening any email attachment unless you were expecting to receive it from that person.
2. Always virus-scan any files downloaded to your computer from any source (CD/DVD, USB hard disks and memory sticks, network files, email attachments or files from the Internet). Virus scans normally happen automatically if your virus definitions are up to date, but you can also initiate manual scans if you wish to be certain.
3. Report any security incidents (such as virus infections) promptly to the IT Helpdesk in order to minimize the damage
4. Respond immediately to any virus warning message on your computer, or if you suspect a virus (e.g. by unusual file activity) by contacting the IT Helpdesk. Do not forward any files or upload data onto the network if you suspect your PC might be infected.

F. Data Backups

1. You will be personally responsible for storing your data in onedrive or Google drive
2. Remember, if the laptop is stolen, lost or damaged, or if it simply malfunctions, it may be impossible to retrieve any of the data from the laptop. Saving the data in one drive will save you a lot of heartache and extra work.

G. Use of Unauthorized Software /Content

1. Employees are required to ensure that they do not download, install or use unauthorized software programs. Unauthorized software could introduce serious security vulnerabilities into the College networks as well as affecting the working of your laptop. Software packages that permit the computer to be ‘remote controlled’ (e.g. PCAnywhere) and ‘hacking tools’ (e.g. network sniffers and password crackers) are explicitly forbidden on the College equipment unless they have been explicitly pre-authorized by the College IT Department.
2. All software or other programs that are downloaded onto the College provided laptop, whether or not they are so downloaded in accordance with the business needs of the College, or the directions of the College management in this regard, shall immediately become the sole and exclusive property of the College, and henceforth can only be used in accordance with the directions of the College in this regard. Further, any programs or software that were pre-installed at the time of the possession of the laptop being handed over to the College, cannot be altered or removed, whether permanently or temporarily, in any manner whatsoever save and otherwise than in accordance with the directions of the College in this regard.
3. As you might expect, the college will not tolerate inappropriate materials such as pornographic, racist, defamatory or harassing files, pictures, videos or

email messages that might cause offence or embarrassment to either the College, its employees or any third party. No employee should ever store, use, copy or circulate such material on the laptop and should not visit or attempt to visit any dubious websites.

4. Employees are also advised that any information in digital or electronic form that they come across in the laptop computer systems provided to them, whether at the time of receiving such systems or at any time thereafter, shall be compulsorily treated by employees as confidential information ("Confidential Information"). Such Confidential Information can exist in any electronic form, including but not limited to documents, memoranda, spreadsheets, databases, encrypted data, passwords, lists of any nature, source code, object code, algorithms, software programs, emails and other communications, designs, blueprints, business projections and plans, financial data, customer and client names and contacts, supplier names and contacts, price lists and quotations, contractual documents, term sheets and executed agreements with vendors/suppliers and customers, and so on. Employees cannot use such Confidential Information in any manner whatsoever save and otherwise than in strict accordance with the directions of the College on this behalf. Any unauthorized usage by the employee of such Confidential Information, or any act of omission or commission of the employee which results in such unauthorized usage of Confidential Information by any third party, shall expose the employee concerned to liability and consequent action by the College and/or its management.
5. Further, in the event any employee is unsure of the status of any digital/electronic information that he or she may discover on any laptop system provided to such employee, the employee must forthwith and without any further delay communicate the existence of such information to the College's IT team on the assumption that all such information is potentially Confidential Information, and thereafter follow the instructions of the IT team

in this regard. Under no circumstances shall the employee attempt to process such Confidential Information in any manner whatsoever for his or her own personal usage, and any delay in contacting the IT team in this regard shall be regarded as dereliction of duty by the employee.

H. CONSEQUENCES OF BREACH

1. Any action of the employee that are inconsistent with this Policy shall be treated as serious professional misconduct on the part of the employee, and the employee concerned shall be subject to any disciplinary proceeding, or action, by the College, which the management of the College may deem appropriate under the existing circumstances. Such action may also include any rights of termination or any other rights that the College may have under the terms of the employment agreement entered into by the College with the employee concerned.
2. Employees are further advised that in the event any such employee fails to adhere to the requirements of laptop usage and restrictions on usage of Confidential Information and proper use, he or she shall be subject to any penal liability under the provisions of the Computer Crimes Act.
3. The College shall bear expenses for laptop maintenance and repairs arising out of the normal wear and tear However, in the event of any damage to the laptop arising out of the negligence, misuse or abuse of the laptop by the employee, the employee shall be solely liable to make the payment for all the expenses arising therefrom.

Brand/Model ____________________

Colour: ________________________

Serial #__________________________

ACCEPTANCE OF TERMS AND CONDITIONS

I ___________________________have read, understood the laptop usage policy

Mobile # ____________________

Signature_____________________________ Date__________________

Position_________________________________

Department _________________________________